
CONFIDENTIAL COMPLIANCE DOCUMENT

UK AI Compliance — Complete

Prepared exclusively for Marchwood Talent

UK Jurisdiction · 11 August 2026



CONTENTS

What is in this pack

Each document below is also attached to your delivery email as its own PDF and editable Word file, so you can circulate or sign any one of them on its own.

Document	What it is for
UK GDPR Gap Analysis for AI Tools	Your AI tools measured against UK GDPR: what is satisfied, what is not, and what closing each gap takes.
AI Acceptable Use Policy	Your formal AI policy. Sign it, circulate it to every member of staff, and review it annually or whenever your AI tool usage changes.
Employee AI Guidelines — Practical Dos and Don'ts	The working-level guidance that sits under the policy: concrete examples of good and bad AI use in this business.
ICO Framework Self-Assessment	The regulator's own framework, worked through and answered.
Compliance Roadmap	The sequence to work through. Do not start a phase until the one before it is complete — the order is deliberate.
Data Classification Matrix	Which categories of your data may go near an AI tool, and which may never. The one page staff refer to before pasting anything in.
GDPR Compliance Position	Your documented data protection position for each AI tool — what a customer's procurement team asks for.
Employee AI Policy Acknowledgement Form	Each member of staff signs one. Keep the signed copies — they are your evidence that the policy was communicated, which is the first thing asked for after an incident.
Full ICO AI Auditing Framework Assessment	The detailed assessment against the regulator's auditing framework — the document to produce if you are ever audited.
Employment AI Procedures	Using AI in recruitment, monitoring or management decisions — the highest-risk use in most businesses, and the most regulated.
Automated Decision-Making Notices and Opt-Out Procedures	The notices you give when a decision is made by a machine, and the route out that the law requires you to offer.
Data Subject Rights Procedures for AI-Processed Data	How you answer an access, correction or deletion request when the data has passed through an AI system.
Sector-Specific Obligations Review	The rules that apply because of the sector you are in, on top of the general AI and data regime.
AI Risk Register	The ongoing record of AI risks, their owners and their mitigations. A live document — review it on the cadence stated at the foot.
AI Incident Response Procedure	What happens in the first hour after an AI-related incident, and who does it. The regulator clock starts before anyone has decided who is in charge.

Also included with your purchase

- Policy review after 12 months, included in the price
- Staff briefing session (60 minutes, remote)

Reply to your delivery email to arrange these.

PART 1

Your AI Compliance Profile

Marchwood Talent is a UK-based recruitment firm (11–50 employees) operating in financial services and healthcare, sectors where candidate data routinely includes special category information such as health declarations and criminal record disclosures under UK GDPR Article 9 and the Rehabilitation of Offenders Act. Their applicant tracking system (ATS) automatically ranks and shortlists candidates before any consultant review, constituting solely automated decision-making with legal or similarly significant effect under UK GDPR Article 22 and the Data (Use and Access) Act 2025 Part 5 safeguards in force since 5 February 2026. Consultants are also pasting CVs containing personal and special category data into ChatGPT without any documented lawful basis, data processing agreement, or data transfer safeguard, creating acute UK GDPR Articles 5, 6, 9, 28, and 44 exposure. The business has no AI policy, no approved-tools register, and no record of data protection impact assessments, meaning it is currently non-compliant across multiple simultaneous legal obligations with maximum ICO fines reaching £17.5 million.

Maximum Fine Exposure

The maximum financial penalty available to the ICO for serious UK GDPR infringements is £17,500,000 or 4% of total annual worldwide turnover for the preceding financial year, whichever figure is higher (s.157 Data Protection Act 2018 as amended). Marchwood Talent has 11–50 employees and has not disclosed its annual turnover; the turnover-based limb of the calculation cannot be computed without that figure. However, the statutory floor of £17,500,000 is available to the ICO regardless of turnover if a Tier 1 infringement is found. On current facts, Marchwood faces exposure across multiple concurrent, independently actionable breaches: (1) ATS automated decision-making with no Article 22 / DUAA 2025 Part 5 safeguards in place since at least 5 February 2026; (2) processing special category health and criminal record data through ChatGPT without an Article 9(2) condition, Schedule 1 DPA 2018 condition, APD, or Article 28 DPA; (3) unlawful international transfers of special category data to OpenAI under Article 44; (4) absence of DPIAs required by Article 35; (5) no complaints procedure under the DUAA 2025 duty in force since 19 June 2026. The ICO's November 2024 recruitment AI audit findings mean Marchwood cannot credibly claim ignorance of sector-specific expectations. Each breach could individually attract a penalty notice; the ICO may assess them as part of a single investigation but is not required to cap aggregate exposure at one penalty. In practical terms, for a firm of this size, even a mid-range ICO penalty in the tens or hundreds of thousands of pounds — comparable to the £247,590 MediaLab.AI penalty — could be existentially significant, without the ICO needing to approach the £17,500,000 statutory ceiling.

AI Tools Inventory

Tool	Use	Risk Level	Notes
ATS with automated candidate ranking and shortlisting	HR, recruitment — automatically scores and shortlists candidates before consultant review	High	Automated ranking before any human review is likely 'solely automated decision-making with significant effect' under UK GDPR Article 22 and the Data (Use and Access) Act 2025 Part 5 (in force 5 February 2026). Candidates in financial services and healthcare roles are profoundly affected by shortlisting outcomes. Marchwood must identify a lawful basis under the DUAA 2025 expanded Article 22 framework, implement mandatory safeguards (right to human review, to contest, to explanation), and conduct a DPIA under UK GDPR Article 35. The ATS vendor

Tool	Use	Risk Level	Notes
			must be covered by an Article 28 data processing agreement. Bias auditing is required under the UK Equality Act 2010 given the risk of algorithmic discrimination on protected characteristics. The ICO published recruitment AI audit outcomes in November 2024 flagging exactly this scenario.
ChatGPT / OpenAI	Consultants paste candidate CVs to generate summaries; ad hoc use with no policy	Unacceptable	Pasting CVs — which include names, contact details, employment history, and in healthcare/financial services roles may include health declarations and criminal record data — into ChatGPT without a data processing agreement breaches UK GDPR Article 28. Sending such data to OpenAI's servers without a lawful basis and appropriate Article 46 transfer mechanism likely breaches Articles 6, 9, and 44. Processing special category data (health, criminal records) requires an Article 9(2) condition and, for criminal data, Schedule 1 DPA 2018 conditions. No organisational authorisation exists, making this shadow AI. This practice must be suspended immediately pending a DPIA, vendor DPA, and approved-use policy. Risk rated Unacceptable because the harm is current, ongoing, and involves special category data with no controls whatsoever.
Microsoft 365 Copilot	Creating marketing and communications content; likely also used across email and documents touching candidate data	High	Microsoft 365 Copilot processes data within the Microsoft tenant and is covered by Microsoft's data processing addendum, which partially mitigates Article 28 risk — but only if Marchwood has reviewed and accepted those terms and configured privacy settings appropriately (e.g., disabling training on tenant data). If Copilot surfaces or processes candidate or client personal data held in SharePoint, Teams, or Outlook, that processing requires a lawful basis and must be disclosed in privacy notices. Given no AI policy exists, it is unknown whether these configurations have been made. A configuration audit and DPIA are required. Risk is High rather than Unacceptable because a vendor DPA framework exists in principle, but current governance gaps leave it unverified.
AI in HR or recruitment systems	HR, recruitment, or performance management functions beyond the ATS ranking	High	Any AI-driven features within HR platforms (e.g., performance scoring, engagement analytics, or candidate communication automation) that produce outputs affecting employees or candidates engage UK GDPR Articles 5, 6, 9, and 22, the DUAA 2025 Part 5 safeguards, and the Equality Act 2010. No inventory of which HR system AI features are active has been noted. Marchwood must audit all active AI features, assess each for automated-decision-making significance, obtain or verify Article 28 agreements, and document lawful bases. Special category data processed by these systems (health, criminal records for healthcare/financial services placements) requires explicit Article 9(2) conditions.

Tool	Use	Risk Level	Notes
AI-powered CRM or sales tools	Data analysis, business intelligence, and sales pipeline management	Limited	Where CRM AI features operate only on business contact data (name, job title, employer) for sales purposes, the risk is lower, but UK GDPR Articles 5, 6, and 13/14 transparency obligations still apply. If candidate personal data flows into the CRM (e.g., contact records for placed candidates), special category considerations re-emerge. The vendor must be covered by an Article 28 DPA. The primary risk here is that no approved-tools register exists, so it is unconfirmed whether the current CRM vendor has a compliant DPA in place. A vendor review and privacy notice update are required.

Applicable Regulations

UK GDPR — Articles 5, 6, 9, 13, 14, 22, 28, 35, 44

The primary UK data protection framework. Article 5 requires lawfulness, fairness, transparency, and data minimisation — pasting CVs into ChatGPT without controls breaches multiple principles simultaneously. Article 6 requires a lawful basis for all processing; Article 9 requires an additional explicit condition for special category data (health, criminal record information) which Marchwood routinely handles for healthcare and financial services candidates. Article 22 restricts solely automated decisions with significant effect and mandates human review, explanation, and contestation rights — directly engaged by the ATS ranking system. Article 28 requires a written data processing agreement with every processor, including ChatGPT/OpenAI and all HR/CRM vendors. Article 35 mandates a DPIA before high-risk processing, including large-scale special category data and automated decision-making. Articles 13–14 require transparent privacy notices disclosing AI-based processing. Article 44 prohibits international transfers without an adequacy decision or appropriate safeguard.

Key date: In force — retained and amended post-Brexit; continuously applicable · Max penalty: £17.5 million or 4% of global annual turnover, whichever is higher (s.157 DPA 2018 as amended)

Data (Use and Access) Act 2025 — Part 5 automated decision-making safeguards

Amends UK GDPR Article 22 to expand lawful bases for solely automated decisions, including a new basis where the controller implements 'appropriate safeguards.' Those safeguards — including the right to human review, to contest a decision, and to obtain an explanation — became legally mandatory on 5 February 2026. Marchwood's ATS shortlisting falls squarely within scope: it makes consequential decisions about candidates (whether they are seen by a consultant at all) using solely automated means. The Act also introduced a duty on controllers to operate a complaints procedure and respond to data protection complaints within set time limits, in force from 19 June 2026. Marchwood has no complaints procedure documented. The Act's expanded bases for research and public-interest processing do not relieve recruitment firms of their core automated-decision-making obligations.

Key date: Part 5 data protection provisions (automated decision-making safeguards): 5 February 2026. Complaints procedure duty: 19 June 2026. · Max penalty: Enforcement via UK GDPR penalty regime: £17.5 million or 4% of global annual turnover

ICO Audit and Accountability Framework — Recruitment AI (November 2024 outcomes)

The ICO published findings from its audit of AI tools in recruitment in November 2024, identifying as key risks: lack of bias testing in automated shortlisting tools, absence of DPIAs, failure to disclose automated processing in privacy notices, and use of AI tools without vendor DPAs. These findings are directly mirrored in Marchwood's current position. While not a statutory instrument, ICO audit outcomes inform enforcement priorities and are treated as indicators of expected standards. Non-compliance with ICO guidance following published sector findings increases regulatory exposure and reduces the credibility of any 'reasonable steps' defence.

Key date: ICO recruitment AI audit outcomes published November 2024 · Max penalty: N/A as a framework document; enforcement under UK GDPR penalties above

UK Equality Act 2010 — ss.4, 13, 19, 39, 41

Prohibits direct discrimination (s.13) and indirect discrimination (s.19) on protected characteristics including race, sex, age, disability, and religion in recruitment (s.39). An ATS that ranks candidates using criteria correlated with protected characteristics — even unintentionally — can constitute indirect discrimination if the provision, criterion, or practice puts a group at a particular disadvantage and is not a proportionate means of achieving a legitimate aim. Marchwood places into healthcare and financial services, sectors with specific diversity obligations. No bias audit of the ATS has been conducted. Employer liability attaches under s.41 for discriminatory acts by agents, which may extend to discriminatory AI vendor outputs. The Equality and Human Rights Commission (EHRC) has concurrent enforcement powers.

Key date: In force — continuously applicable · Max penalty: Employment tribunal awards are uncapped for discrimination claims; EHRC can seek injunctions and compliance notices; reputational and client relationship risk is severe in regulated-sector placements

UK GDPR Article 44 and international data transfers

Transfers of personal data to countries outside the UK require either an adequacy regulation or appropriate safeguards such as UK International Data Transfer Agreements (IDTAs) or UK Addendum to EU SCCs. OpenAI processes data on US-based infrastructure. The UK–US data bridge (adequacy decision) applies only to US organisations certified under it. Marchwood must verify whether OpenAI is covered by an applicable transfer mechanism before any personal data — let alone special category data — is sent via ChatGPT. Current practice of pasting CVs into ChatGPT has no documented transfer basis, constituting an unlawful transfer under Article 44.

Key date: UK–US Data Bridge in force October 2023; ongoing obligation · Max penalty: Captured within the UK GDPR £17.5 million / 4% turnover penalty regime

DPA 2018 — Schedule 1 conditions for criminal conviction and offence data

Processing criminal record data (which Marchwood handles for financial services and healthcare placements) requires not only an Article 9 equivalent condition but also a Schedule 1, Part 2 DPA 2018 condition and an appropriate policy document (APD) under Schedule 1, Part 4. The APD must describe how the business complies with the data protection principles and its retention and erasure policies for that data. Running criminal record data through an ATS or pasting it into ChatGPT without an APD in place is a distinct statutory breach beyond the core UK GDPR violations.

Key date: In force — continuously applicable · Max penalty: Criminal data breaches captured within UK GDPR penalties: £17.5 million or 4% global turnover

UK GDPR Gap Analysis for AI Tools

Your AI tools measured against UK GDPR: what is satisfied, what is not, and what closing each gap takes.

Requirement	Article	Tool / Scope	Current Position	Gap	Action	Priority
GAP COUNT SUMMARY	—	All tools	Critical: 9 High: 8 Medium: 4 Low: 1	22 gaps identified across 8 requirement areas and 5 tools	Resolve Critical gaps before processing any further candidate data	SUMMARY
Lawful basis — special category data (health declarations)	UK GDPR Art 9(2); DPA 2018 Sch 1	ATS; ChatGPT	No explicit Art 9 condition identified or documented for processing health data in candidate records	No lawful basis for special category processing. ICO can order immediate cessation.	Identify and document an Art 9(2) condition (e.g. Sch 1 para 1 employment condition) before next candidate intake.	Critical
Lawful basis — special category data (criminal records)	UK GDPR Art 10; DPA 2018 s 11 & Sch 1	ATS; ChatGPT	Criminal record declarations processed with no documented Art 10 condition or DPA 2018 Sch 1 condition in place	Unlawful processing of criminal record data. Maximum ICO fine £17.5m or 4% global turnover.	Document an appropriate Sch 1 condition (e.g. para 2 — substantial public interest) and obtain DPO or legal sign-off.	Critical
Lawful basis — standard personal data	UK GDPR Art 6(1)	ATS; ChatGPT; Copilot; CRM; HR system	No lawful basis register exists. Legitimate interests assessment (LIA) not conducted for any tool.	All AI-assisted processing currently lacks documented Art 6 basis. Systemic gap across all tools.	Complete lawful basis register and LIA for each tool within 30 days. Assign data owner to maintain it.	Critical
Transparency — privacy notice (candidates)	UK GDPR Arts 13–14	ATS; ChatGPT; CRM	No privacy notice discloses AI-assisted shortlisting, CV summarisation via ChatGPT, or CRM profiling.	Candidates unaware of AI processing. ICO audit finding likely if investigated.	Update candidate privacy notice to name each AI tool, its purpose, and the logic of automated ranking.	Critical
Transparency — privacy notice (placed workers)	UK GDPR Arts 13–14	HR system; Copilot	No notice covers AI use in performance management or comms drafting involving personal data.	Placed workers and contractors lack information required by Art 13.	Add AI processing disclosures to worker on-boarding documentation and the existing HR privacy notice.	High
Requirement	Article	Tool / Scope	Current Position	Gap	Action	Priority
Automated decision-making — ATS ranking/shortlisting	UK GDPR Art 22; DUAA 2025 Part 5 (in force 5 Feb)	ATS	ATS ranks and shortlists candidates before any consultant	Solely automated decisions producing legal or similarly	Map the ATS decision logic. Implement human meaningful review	Critical

Requirement	Article	Tool / Scope	Current Position	Gap	Action	Priority
	2026)		review. No Art 22 safeguards in place.	significant effects are unlawful without DUAA safeguards.	before shortlist is acted on, or invoke a DUAA lawful basis with full safeguards.	
Automated decision-making — right to explanation and contest	UK GDPR Art 22(3); DUAA 2025 Part 5	ATS	Candidates have no mechanism to request human review, explanation, or to contest ATS rankings.	Breach of Art 22(3) rights. ICO enforcement likely given November 2024 recruitment AI audit findings.	Create and publicise a candidate contest procedure. Log all requests and outcomes.	Critical
Automated decision-making — DUAA complaints procedure	DUAA 2025 (in force 19 Jun 2026)	ATS; HR system	No complaints procedure exists. No defined response timeframes for data protection complaints.	Duty to operate complaints procedure with set time limits has applied since 19 June 2026. Marchwood is currently non-compliant.	Draft and publish an AI/data protection complaints procedure. Set response SLA aligned to DUAA requirements.	Critical
Bias and equality — algorithmic fairness	UK Equality Act 2010 ss 4, 19; UK GDPR Art 22(3)	ATS	ATS ranking algorithm untested for disparate impact across protected characteristics. No audit trail.	Indirect discrimination risk. ICO and EHRC both have enforcement remit. Healthcare and financial services placements increase scrutiny.	Commission or conduct an algorithmic bias audit of the ATS. Document results and corrective action.	Critical
Data minimisation	UK GDPR Art 5(1)(c)	ChatGPT; Copilot	Consultants paste full CVs (including health and criminal data) into ChatGPT. Copilot may ingest full HR records.	Excessive personal data — including special category — sent to third-party AI with no minimisation controls.	Issue a standing instruction: redact name, health, and criminal data before any CV enters ChatGPT or Copilot.	Critical
Data transfer — ChatGPT / OpenAI	UK GDPR Arts 44–46; UK Adequacy Regulations	ChatGPT	OpenAI processes data on US infrastructure. No evidence of UK transfer mechanism (IDTA or equivalent) reviewed or signed.	International transfer of special category candidate data without a compliant transfer mechanism.	Review OpenAI DPA, confirm IDTA or UK adequacy basis, and record the transfer mechanism in the data register.	High
Requirement	Article	Tool / Scope	Current Position	Gap	Action	Priority
Shadow AI — unauthorised tools	UK GDPR Art 5(1)(f); Art 28	Any unapproved tool	No approved-tools list exists. Consultants are known to use	Uncontrolled personal data leaving Marchwood	Publish an approved-tools register. Prohibit unapproved AI	High

Requirement	Article	Tool / Scope	Current Position	Gap	Action	Priority
			ChatGPT ad hoc. Other shadow tools cannot be ruled out.	systems to unvetted processors. No Art 28 processor agreement possible without known tools.	tools in a written policy. Conduct a staff self-declaration exercise.	
Processor agreements	UK GDPR Art 28	ChatGPT; Copilot; ATS; CRM; HR system	No record that Data Processing Agreements (DPAs) are in place or have been reviewed for any AI tool.	Processing by sub-processors without compliant Art 28 contracts is a standalone GDPR breach.	Obtain and file DPAs for all five tools. Document sub-processor chains, especially for OpenAI and Microsoft.	High
Accuracy	UK GDPR Art 5(1)(d)	ChatGPT; ATS	AI-generated CV summaries and ATS rankings are not verified for accuracy before influencing consultant decisions.	Inaccurate profiles may lead to discriminatory shortlisting and breach Art 5(1)(d).	Require consultants to verify AI summaries against source CV before recording or acting on them.	High
Storage limitation — candidate data in AI tools	UK GDPR Art 5(1)(e)	ChatGPT; Copilot; CRM	No retention schedule covers data held within AI tool logs, CRM AI features, or Copilot conversation history.	Special category data retained indefinitely in AI tool logs with no deletion mechanism.	Map where AI tools retain data. Configure retention/deletion settings and include in the data retention schedule.	High
Storage limitation — ATS records	UK GDPR Art 5(1)(e)	ATS	No documented retention period for unsuccessful candidate profiles held in the ATS.	ICO guidance requires defined retention for unsuccessful applicants, typically 6–12 months.	Set and enforce an ATS retention period. Automate deletion or flag for review at period end.	High
Security — special category data in ChatGPT	UK GDPR Art 32	ChatGPT	Health and criminal record data pasted into ChatGPT with no encryption, access control, or security assessment.	Foreseeable high-risk breach of Art 32. OpenAI's default model-training opt-outs not confirmed as applied.	Confirm OpenAI enterprise settings disable training on Marchwood data. Prohibit special category data in ChatGPT pending assessment.	High
Security — access controls across tools	UK GDPR Art 32	ATS; CRM; HR system; Copilot	No evidence of role-based access controls or regular access reviews for AI-enabled tools.	Excessive access increases insider risk and breach severity.	Implement least-privilege access. Conduct access review quarterly. Log access to special category data fields.	Medium

Requirement	Article	Tool / Scope	Current Position	Gap	Action	Priority
Accountability — DPIA	UK GDPR Art 35; ICO AI Auditing Framework	ATS; ChatGPT	No Data Protection Impact Assessment conducted for ATS automated ranking or ChatGPT CV processing. Both are high-risk.	Mandatory DPIA requirement triggered by Art 35(3)(a) (automated decisions) and Art 35(3)(b) (special category at scale).	Complete DPIAs for ATS and ChatGPT before next candidate intake. Consult ICO if residual risk remains high.	Critical
Accountability — AI governance policy	UK GDPR Art 5(2); ICO AI Auditing Framework	All tools	No AI policy, no approved-tools list, no governance framework. Confirmed by client notes.	Inability to demonstrate accountability under Art 5(2). ICO's first question in any audit.	Produce and adopt an AI Acceptable Use Policy covering all five in-scope tools within 30 days.	High
Accountability — staff training	UK GDPR Art 5(2); Art 32	All tools	No training on AI data risks, bias, or lawful CV processing. Consultants paste special category data into ChatGPT without awareness of risk.	Human error is the most common cause of breaches. Untrained staff = uncontrolled risk.	Deliver mandatory AI and data protection training to all consultants before next candidate intake.	Medium
Accountability — records of processing	UK GDPR Art 30	All tools	No Article 30 record of processing activities (ROPA) covers AI tools or special category data flows.	Fundamental accountability breach. ROPA is an ICO audit starting point.	Update ROPA to include all AI tools, data categories, purposes, transfers, and retention periods.	Medium
Sector-specific risk — financial services placements	ICO AI Auditing Framework; FCA expectations	ATS; ChatGPT	No enhanced controls for candidates placed into FCA-regulated roles despite higher data sensitivity and regulatory scrutiny.	FCA-regulated client firms may require evidence of Marchwood's data governance before accepting referred candidates.	Add a flag in the ATS for FS placements. Apply stricter access and retention controls to those records.	Medium

RATING SCALE — Critical: regulatory breach active now, cessation or enforcement risk imminent. High: breach likely or near-certain without remediation within 60 days. Medium: control weakness requiring action within 90 days. Low: best practice enhancement; no immediate breach risk.

MAXIMUM FINE EXPOSURE — The ICO may impose fines up to £17.5 million or 4% of global annual turnover, whichever is higher. The turnover-based limb cannot be calculated without Marchwood Talent's audited annual revenue figures. The gaps identified in this analysis, particularly unlawful special category processing (Arts 9 and 10), absent Art 22 safeguards, and missing DPIAs, each constitute standalone infringements capable of attracting the upper tier of fines.

DUAA 2025 POSITION — Part 5 data protection provisions, including the expanded lawful bases for solely automated decisions and their associated safeguards, came into force on 5 February 2026. The duty to operate a complaints procedure and respond

within set time limits came into force on 19 June 2026. Both apply to Marchwood Talent now. The DUAA does not remove the Art 22 requirement for human review; it provides a framework within which automated decisions may be lawful if the conditions and safeguards are met.

CHATGPT / OPENAI — Marchwood must operate under OpenAI's enterprise or API tier with a signed Data Processing Agreement and model-training-on-inputs disabled. The free or standard consumer tier does not provide the Art 28 processor agreement required for any personal data processing, let alone special category data. This must be resolved before the next use of the tool.

ATS AUTOMATED RANKING — The ICO published recruitment AI audit outcomes in November 2024. The ICO's stated position is that where an ATS produces a ranked shortlist that a recruiter then acts on without genuinely reviewing the underlying data, this is likely a solely automated decision under Art 22 regardless of nominal human involvement. Marchwood must obtain and review the ATS vendor's documentation of the ranking logic, protected-characteristic inputs, and bias-testing history.

SPECIAL CATEGORY DATA IN HEALTHCARE AND FINANCIAL SERVICES PLACEMENTS — Criminal record and health declaration data are Art 9 and Art 10 data. Processing them through ChatGPT's standard interface, or retaining them in an ATS without an identified Sch 1 DPA 2018 condition, is unlawful today. This is the single highest-risk finding in this analysis.

REVIEW CADENCE — This gap analysis should be reviewed quarterly and updated whenever a new AI tool is introduced, an existing tool's functionality changes materially, or the ICO publishes updated guidance on recruitment AI. Owner: Data Protection lead / DPO (to be appointed if not already in post).

DOCUMENT OWNER — Marchwood Talent compliance lead. Date of analysis: 11 August 2026.

AI Acceptable Use Policy

Your formal AI policy. Sign it, circulate it to every member of staff, and review it annually or whenever your AI tool usage changes.

AI Acceptable Use Policy — Marchwood Talent

Version 1.0 | Effective Date: 11 August 2026 | Policy Owner: [Name of designated senior responsible person, e.g. Managing Director or Head of Operations]

This policy is issued under the authority of the Marchwood Talent senior leadership team. It is a mandatory document. Every member of staff must read it, confirm they have understood it, and comply with it in full from the date it is circulated. It is reviewed annually and whenever the company's AI tool usage materially changes.

1. Scope — People, Tools and Activities Governed

This policy applies to every individual who works for or on behalf of Marchwood Talent, including permanent employees, temporary workers, contractors engaged on Marchwood's own contracts, and any third-party supplier or partner who accesses Marchwood systems or data in the course of providing services to the business. There are no exceptions based on seniority, job title, or employment status.

The policy governs all use of artificial intelligence tools and AI-assisted features in the course of Marchwood Talent's business activities. The tools currently in scope are: (a) the applicant tracking system (ATS) that includes automated candidate ranking and shortlisting functionality; (b) ChatGPT and other OpenAI products, whether accessed via browser, API or third-party integration; (c) Microsoft 365 Copilot, including its integration within Outlook, Word, Excel, Teams and any other Microsoft 365 application; (d) any AI functionality embedded within Marchwood's HR or recruitment platform; and (e) any AI-powered CRM or sales tool in use by the business.

The activities governed include, but are not limited to: processing or summarising candidate CVs or profiles; ranking, scoring or shortlisting candidates for roles; drafting job advertisements, client communications, marketing content or internal documents; analysing business or workforce data; and any other task where an AI tool generates, refines or informs output that is used in Marchwood's work. This policy applies whether a tool is accessed from a Marchwood device, a personal device, a client's premises, or any remote location.

2. Approved Tools and the Process for Requesting a New Tool

The approved AI tools for Marchwood Talent are those listed in Section 1 above. No other AI tool may be used for any business purpose. The use of AI tools not on the approved list — whether free consumer tools, browser extensions, third-party plugins, or any other AI-enabled service — is prohibited. This prohibition addresses the specific risk of shadow AI: staff obtaining AI assistance through channels that Marchwood has not assessed, contracted for, or brought within its data protection and compliance framework.

If a member of staff identifies an AI tool they believe would benefit the business, they must submit a written request to the Policy Owner before using it for any business purpose. The request must name the tool, describe its intended use, identify what categories of data would be entered into it, and provide the supplier's privacy notice and data processing terms. The Policy Owner will assess the request against the criteria in this policy — particularly data protection obligations under UK GDPR, the requirements of the Data (Use and Access) Act 2025, and equality and bias risks under the Equality Act 2010 — and will return a written decision within ten working days. A tool is not approved until the Policy Owner confirms approval in writing and the tool is added to the approved list. Using a tool in the interim period, or after a request has been refused, constitutes a policy breach under Section 8.

3. What May Never Be Entered Into an AI Tool

Certain categories of information are absolutely prohibited from being entered into any AI tool, whether approved or not, unless Marchwood has in place a specific data processing agreement with the tool provider that lawfully covers that data type, and the Policy Owner has confirmed in writing that the specific use is permitted. The absolute prohibitions are as follows.

Personal data of candidates, placed workers, clients or Marchwood staff may not be pasted, typed or uploaded into any AI tool. This includes names, contact details, national insurance numbers, dates of birth, addresses, employment history, salary information, references, or any other information that identifies or could identify a living individual. Marchwood handles criminal record disclosures and health declarations for candidates placed into financial services and healthcare roles. These are special category personal data under UK GDPR Article 9 and criminal conviction data under Article 10. They attract the highest level of legal protection and must never be entered into any AI tool under any circumstances. The ICO has made clear in its recruitment AI audit outcomes (November 2024) that processing sensitive candidate data through external AI tools without appropriate safeguards exposes organisations to serious enforcement risk.

In practical terms, this means consultants must not paste a candidate's CV into ChatGPT or any other AI tool. This practice has been identified as occurring at Marchwood and it stops with immediate effect from the date this policy is circulated. If a consultant needs to summarise a CV, they must do so manually, or use a tool that processes only anonymised data where a specific written permission from the Policy Owner has been granted.

Confidential client information, including client briefs, fee arrangements, shortlisting criteria, salary bands and any information shared under a non-disclosure agreement, may not be entered into any AI tool. Credentials — including usernames, passwords, API keys and authentication tokens — must never be entered into any AI tool. Any draft document that contains client-identifiable information must be anonymised before AI assistance is sought in drafting or editing it.

4. Verification of Output Before Use and Responsibility When Output is Wrong

All AI-generated output must be reviewed and verified by a qualified human member of staff before it is used internally for a material decision, sent to a candidate, shared with a client, or published in any form. Verification means actively checking the substance of the output for accuracy, relevance, absence of bias, and compliance with this policy. It does not mean reading the output once and assuming it is correct because it appears fluent and confident. AI tools, including those approved under this policy, are known to produce plausible-sounding but factually incorrect, outdated or biased results.

The consultant or member of staff who submits the output for use — whether by sending an email, publishing content, incorporating a summary into a candidate record, or using AI-ranked output to make a recommendation — is personally responsible for its accuracy and compliance. Approval by a line manager does not transfer that responsibility unless the line manager has independently verified the output themselves. If AI is used to draft a client communication, the sender owns it. If a consultant uses an AI summary of a candidate profile to brief a client, the consultant is accountable for any error in that summary.

The Pinsent Masons case (May 2026), in which a court criticised a law firm for false submissions based on AI-generated search results, illustrates the professional and legal consequences of failing to verify AI output. Marchwood operates in financial services and healthcare recruitment, sectors with heightened regulatory scrutiny. An unverified AI error that affects a candidate's prospects or misleads a regulated client employer carries reputational and legal risk far beyond the cost of thorough human review.

5. Where a Human Decision is Mandatory

Marchwood's ATS ranks and shortlists candidates automatically before a consultant sees them. This process constitutes automated decision-making within the meaning of UK GDPR Article 22 and the Data (Use and Access) Act 2025. Where that automated process produces a result that has a significant effect on a candidate — including whether they proceed to the next stage of a selection process, are presented to a client, or are removed from consideration — a human consultant must independently review the ranked output and form their own substantive judgement before any such outcome is communicated to the candidate or acted upon.

Automated ranking scores and shortlisting outputs produced by the ATS are advisory inputs, not decisions. No candidate may be rejected, progressed or presented to a client solely on the basis of an ATS-generated score without a consultant reviewing the underlying profile and confirming the outcome. This requirement is mandatory and applies to every vacancy, regardless of volume. The fact that the ATS may process hundreds of applications does not reduce the obligation; it requires Marchwood to resource its consulting capacity accordingly.

Candidates for roles in financial services and healthcare will frequently have disclosed health information or criminal record data as part of pre-employment checks. Decisions affecting those candidates — including whether to present them, how to present them, or whether their disclosures affect their suitability — must always be made by a named human consultant who has reviewed the relevant information directly, without delegating the assessment to an AI tool. Human decision-making is also mandatory in any situation involving a candidate complaint about AI-generated output or ATS ranking, any escalation under the candidate-facing complaints procedure required by the Data (Use and Access) Act 2025 (in force 19 June 2026), and any situation where a consultant believes the AI output may reflect a discriminatory pattern under the Equality Act 2010.

6. Disclosure — Telling Candidates and Clients When AI Was Used

Marchwood will be transparent with candidates and clients about the role AI plays in its processes. This is both an ethical commitment and a legal obligation. UK GDPR Articles 13 and 14 require data controllers to provide meaningful information about automated decision-making, including the logic involved and the significance of the processing for the individual. The Data (Use and Access) Act 2025 reinforces and extends these obligations in the context of automated decisions.

Marchwood's candidate-facing privacy notice must be updated to explain clearly that the ATS uses automated ranking and shortlisting functionality, that this is one input into a consultant's review and not a final decision, and that candidates have the right to request a human review of any outcome and to raise a complaint through Marchwood's complaints procedure. The complaints procedure must meet the requirements of the Data (Use and Access) Act 2025, which has required controllers to operate a complaints procedure and respond within set time limits since 19 June 2026. The Policy Owner is responsible for ensuring the privacy notice and complaints procedure are compliant before this policy takes effect.

Where Marchwood uses AI to draft a communication sent to a candidate or client in Marchwood's name — such as a marketing email, a role briefing, or a newsletter — and where the AI contribution was substantial rather than a minor editing aid, Marchwood will include a brief disclosure in the communication or in its standard terms. Where a client specifically asks whether AI was used in a selection process or in producing a document, Marchwood will answer honestly and fully. No member of staff may deny or conceal AI involvement in Marchwood's work when asked directly by a candidate, client or regulator.

7. Record Keeping and Retention for AI-Assisted Work

Marchwood must maintain a record of its AI-assisted activities sufficient to demonstrate compliance with UK GDPR, the Data (Use and Access) Act 2025, and this policy. The ICO's AI Auditing Framework identifies record keeping as a foundational accountability measure, and the ICO's audit of AI in recruitment (November 2024) confirmed that recruitment businesses are expected to document how AI tools are used in selection processes.

For every vacancy where the ATS applies automated ranking or shortlisting, the consultant responsible for the role must record: the date on which the ATS ranking was produced; the names of candidates included in and excluded from the shortlist by the ATS; the consultant's own assessment following human review; any departures from the ATS ranking and the reason for each departure; and the identity of the consultant who made the final shortlisting decision. These records must be retained for the duration of the relevant hiring process and for a minimum of twelve months thereafter, or longer if a complaint or claim is outstanding.

For AI-assisted content creation using Microsoft 365 Copilot, ChatGPT or any other approved tool, staff must note in the relevant file or project record that AI assistance was used and identify the tool. Final outputs must be saved in their verified, human-reviewed form. Draft AI outputs that have not been verified must not be saved as final documents or sent externally.

Records produced under this section may be requested by the ICO in the event of an investigation or audit. Given that Marchwood processes special category data (health declarations) and criminal conviction data in the context of financial services and healthcare placements, the potential regulatory exposure in the event of inadequate records is significant. The maximum fine available to the ICO is £17.5 million or 4% of global annual turnover, whichever is higher; the turnover-based limb cannot be calculated here without Marchwood's figures, but the statutory maximum on the fixed limb alone illustrates the stakes.

8. Breach of This Policy — Reporting Route and Disciplinary Position

Any member of staff who becomes aware that this policy has been breached — whether by themselves, a colleague, or a third party — must report it to the Policy Owner as soon as possible and in any event within 24 hours of becoming aware. If the breach involves the Policy Owner, the report should be made to the most senior available member of the leadership team. A breach includes, but is not limited to: using an AI tool not on the approved list; entering personal data, special category data, criminal conviction data, client confidential information or credentials into any AI tool; sending AI-generated output to a candidate or client without human verification; allowing an ATS ranking to determine a candidate outcome without consultant review; and concealing AI use from a candidate, client or regulator.

Where a breach may constitute a personal data breach under UK GDPR — for example, where a candidate's CV or health declaration has been entered into ChatGPT or another tool whose data processing terms have not been assessed — the Policy Owner must assess within 72 hours whether notification to the ICO is required under UK GDPR Article 33, and whether affected individuals must be notified under Article 34. The 72-hour clock runs from the point at which Marchwood becomes aware of the breach, not from the point of report. This assessment must be documented regardless of whether notification is ultimately made.

Breaching this policy is a disciplinary matter. Depending on the nature and severity of the breach, the consequence may range from a formal written warning to summary dismissal for gross misconduct. In particular, deliberately entering special category or criminal conviction data into an unauthorised AI tool, or deliberately concealing a breach from the Policy Owner, will be treated as gross misconduct. These disciplinary consequences exist alongside, not instead of, any legal liability that may arise under UK GDPR or other applicable law. The existence of a policy breach by an individual does not transfer Marchwood's regulatory liability to that individual; Marchwood as data controller remains accountable to the ICO.

9. Review Cycle, Policy Owner and Signature Block

This policy must be reviewed by the Policy Owner at least once every twelve months from its effective date, and additionally whenever any of the following occur: Marchwood adopts a new AI tool or discontinues an existing one; there is a material change in the regulatory framework applicable to AI in recruitment, including changes to UK GDPR, the Data (Use and Access) Act 2025, or ICO guidance; Marchwood expands into a new sector or begins handling new categories of candidate data; or a policy breach reveals a gap or ambiguity in the policy's terms.

Following each review, the Policy Owner must produce a written record confirming either that the policy remains adequate without amendment, or setting out the amendments made and the reasons for them. Any amended version of this policy must be re-circulated to all staff and a fresh confirmation of understanding obtained.

The named Policy Owner for this version of the policy is the individual identified at the head of this document. The Policy Owner is responsible for maintaining the approved tools list, processing new tool requests, overseeing compliance with this policy, managing the breach reporting and notification process, and liaising with the ICO or other regulators if required. If the named Policy Owner leaves the business or changes role, a replacement must be named in writing within five working days.

By signing below, the Policy Owner confirms that this policy has been approved by Marchwood Talent's senior leadership, that it reflects Marchwood's current AI tool usage and legal obligations as at the effective date, and that it will be circulated to all staff and third parties in scope.

Signed: _____

Name: _____

Title: _____

Date: _____

On behalf of: Marchwood Talent

Employee AI Guidelines — Practical Dos and Don'ts

The working-level guidance that sits under the policy: concrete examples of good and bad AI use in this business.

Introduction and Purpose

These guidelines apply to every Marchwood Talent employee who touches an AI tool, whether as part of an approved workflow or on an ad hoc basis. They translate Marchwood Talent's obligations under UK GDPR Article 22, the Data (Use and Access) Act 2025 (in force from 5 February 2026), the ICO AI Auditing Framework, and the UK Equality Act 2010 into day-to-day working practice. Non-compliance is not a theoretical risk: the ICO can fine up to £17.5 million or 4% of global annual turnover for serious UK GDPR breaches, and the ICO published specific recruitment AI audit outcomes in November 2024 that signal active scrutiny of exactly the tools Marchwood Talent uses.

These guidelines are not aspirational. They describe what you must do and what you must not do. If you are uncertain about a situation not covered here, stop and escalate rather than proceeding on your own judgement.

Approved Tools and the Shadow AI Rule

The only AI tools permitted for work purposes at Marchwood Talent are: the ATS with automated candidate ranking and shortlisting, ChatGPT / OpenAI (via a paid, privacy-preserving account configured by the business), Microsoft 365 Copilot, AI functions within the approved HR or recruitment platform, and the AI-powered CRM. Any other AI tool — including personal free-tier ChatGPT accounts, Gemini, Claude, Perplexity, or any browser-based AI assistant not on this list — is unauthorised and must not be used for any work task.

Do: Before using any AI feature, confirm it appears on the approved list. If a new tool is suggested by a vendor or a colleague, flag it to your line manager before use.

Do not: Paste candidate CVs, client job briefs, salary data, health declarations, criminal record information, or any other work-related content into a personal or unapproved AI account. Even a single CV upload to an unapproved tool is a personal data breach reportable to the ICO within 72 hours under UK GDPR Article 33. Using unauthorised tools is also referred to as 'shadow AI' and is a disciplinary matter at Marchwood Talent.

Worked Example — ATS Automated Candidate Ranking and Shortlisting

Marchwood Talent's ATS scores and ranks candidates automatically before any consultant sees a profile. This is automated decision-making that produces a meaningful effect on a person's job prospects. Under UK GDPR Article 22 and the Data (Use and Access) Act 2025, candidates have the right to obtain human intervention, express their point of view, and contest the decision. The Act's commencement on 5 February 2026 means the updated safeguards for solely automated decisions are already in force.

Do: Treat the ATS ranking as a starting filter, not a final decision. Before removing a candidate from a shortlist, open their full profile and apply your own professional judgement. Document that you reviewed the profile and note the reason for any rejection in the ATS record. If a candidate placed into healthcare or financial services has declared a health condition or criminal record, be particularly careful: the ATS may have weighted these fields in ways that engage the Equality Act 2010 (protected characteristics including disability) and Article 9 UK GDPR (special category health data).

Do not: Accept the ATS rank order without scrutiny and send only top-ranked candidates to a client without independent review. Do not rely on the numeric score alone when placing candidates into regulated sectors. Do not ignore a candidate who contacts you to query why they were not shortlisted — they have a legal right to an explanation and human review, and you must escalate this to a manager immediately.

Worked Example — Pasting CVs into ChatGPT to Summarise Them

Consultants currently paste CVs directly into ChatGPT to generate summaries. This practice, in its current form, is not compliant and must change immediately. A CV is personal data under UK GDPR. When a Marchwood Talent candidate places into healthcare or financial services, their CV may also contain health declarations or criminal record disclosures, which are special category data under Article 9 and criminal offence data under Article 10. Pasting this into any ChatGPT session that has not been configured with an enterprise data processing agreement in place constitutes unauthorised transfer of personal data to a third-party processor without an adequate legal basis.

Do: Use only the business's approved, enterprise-configured ChatGPT account. Before pasting any CV, remove or replace the candidate's full name, address, phone number, email, date of birth, and any explicit health or criminal record text. Use placeholders such as 'Candidate A' and 'redacted health declaration' so that the output cannot be linked back to a real person if the session log were ever accessed. Instruct the tool with a prompt such as: 'Summarise the professional experience and skills in this CV for a financial services compliance role. No personal identifiers are included.' Then review the summary before using it.

Do not: Paste an unredacted CV into any ChatGPT session. Do not paste into a personal free-tier OpenAI account. Do not forward a ChatGPT-generated summary to a client without reading it yourself first — the tool regularly omits material detail or mischaracterises seniority, which would be a misleading representation to the client and could expose Marchwood Talent to liability.

Worked Example — Microsoft 365 Copilot for Marketing and Communications Content

Marchwood Talent uses Microsoft 365 Copilot to draft job advertisements, candidate-facing emails, LinkedIn content, and client communications. This is a lower-risk use in terms of personal data, but it carries specific risks around accuracy, tone, and equality compliance.

Do: Use Copilot to produce a first draft of a job advertisement and then review it against the Equality Act 2010 before publishing. Look specifically for language that may discourage applications from particular groups — phrases like 'energetic young team,' 'native English speaker,' or 'recent graduate' can constitute indirect discrimination. When drafting candidate communications, check that Copilot has not introduced language that implies preference for a particular gender, age group, or nationality. Use a prompt such as: 'Draft a job advertisement for a contract compliance analyst role in financial services. Use inclusive language. Do not reference age, physical ability, or personal background.'

Do not: Publish any Copilot-drafted content directly without a human review step. Do not use Copilot to draft a rejection letter for a specific named candidate and then send it without reading it — Copilot may generate generic language that does not reflect the actual reason for rejection, which could be misleading or discriminatory if challenged. Do not include any candidate's name or personal data in a Copilot prompt unless you have confirmed that your Microsoft 365 tenancy is configured to exclude prompt data from model training.

Worked Example — AI-Powered CRM and Data Analysis

The AI-powered CRM and data analysis tools are used for pipeline reporting, business intelligence, and identifying placement trends. These tools may process personal data about candidates and clients. Their outputs inform business decisions including which candidates to re-engage and which client sectors to prioritise.

Do: When running CRM reports that include individual candidate records, treat the output as personal data. Store outputs in folders with appropriate access controls and do not share them in unprotected email attachments. If the CRM surfaces a recommendation such as 'candidates in this category have a lower placement rate,' investigate the underlying data before acting on it — the pattern may reflect historical bias in your own data rather than candidate quality, and acting on it uncritically could breach the Equality Act 2010.

Do not: Use CRM AI-generated candidate scoring to exclude groups of candidates without reviewing the methodology. Do not export bulk candidate data from the CRM into an external AI tool for analysis — this would be an unauthorised data transfer. Do not treat a CRM prediction about a candidate's likelihood of acceptance as a substitute for speaking to the candidate directly.

Prompting Practice — Avoiding Disclosure of Personal or Client Data

Every time you write a prompt for any AI tool, treat it as if you were sending an email to an unknown external party. Personal data included in a prompt may be retained in logs, used in system diagnostics, or — in unapproved free-tier tools — used to train future models. This is a data protection risk even when using approved tools, and it is a serious breach when using unapproved ones.

The following prompting rules apply across all approved Marchwood Talent AI tools. Before submitting any prompt, ask yourself whether the prompt contains a candidate's real name, contact details, date of birth, NI number, or any reference to health, disability, pregnancy, criminal record, nationality, or religion. If yes, remove or anonymise that information before submitting. Describe the situation in general terms: instead of 'John Smith has declared epilepsy on his health form — how do I handle this placement into an NHS trust?' write 'A candidate for a healthcare contract role has disclosed a health condition. What placement considerations apply under UK employment law?'

When prompting the ATS, CRM, or HR platform, be aware that these systems may log your queries and link them to candidate records. Use the system's intended interface rather than free-text workarounds that bypass audit trails. Always include enough instruction in your prompt to shape the output towards the task — vague prompts produce generic outputs that require more correction and create more risk of a confident, plausible error.

Checking Output for Fabrication, Bias, and Confident Errors

AI tools used by Marchwood Talent, including ChatGPT and Microsoft 365 Copilot, are capable of producing text that is fluent, confident, and factually wrong. This is sometimes called hallucination. In a recruitment context, a hallucinated qualification, an invented employment date, or a fabricated FCA registration number could expose Marchwood Talent to negligence claims, regulatory sanction, or reputational damage with a client operating in a regulated sector.

Do: Treat every AI output as a draft that requires verification, not a finished document. For CV summaries, cross-reference the AI summary against the original CV line by line before the summary is used. For any output that contains a date, qualification, regulatory status, or numerical figure, verify that figure against the source document. For marketing content, check that any claim about Marchwood Talent's services or sector expertise is accurate.

Do not: Forward an AI-generated summary to a client without reading it in full yourself. Do not assume that because the output sounds confident and professional, it is accurate. Do not use AI to draft responses to candidate queries about their ATS outcome, data rights, or complaints without a manager reviewing and approving the response first — a hallucinated explanation of a legal right could constitute a misleading statement to a data subject.

Bias checking is equally important. The ATS ranking algorithm and CRM scoring tools may reflect historical patterns in Marchwood Talent's own data, which may embed demographic skew. If you notice that the ATS consistently ranks candidates from particular universities, geographic areas, or with particular name patterns more highly, this must be escalated immediately as a potential Equality Act 2010 and UK GDPR issue.

Handling AI Output That Will Be Seen by a Candidate or Client

Any communication sent to a candidate or client that was drafted or summarised by an AI tool must pass through a human review step before it leaves Marchwood Talent. This applies to job advertisements, shortlist summaries, rejection communications, placement confirmations, marketing emails, and LinkedIn posts. It also applies to internal briefing notes that will be shared with a client contact.

Do: Read the full draft before sending. Check for accuracy against source documents. Check for tone — AI tools sometimes produce language that is blunt, condescending, or oddly formal in a way that does not reflect Marchwood Talent's voice. Check for equality compliance as described in the marketing section above. If the communication relates to a candidate's application outcome, ensure the stated reason for any decision is accurate and can be substantiated, because the candidate may request access to it under UK GDPR Article 15 or challenge it under Article 22.

Do not: Auto-send any AI-generated email without human approval. Do not use AI to generate a personalised rejection for a specific candidate without substituting accurate information about their actual application. Do not allow a Copilot draft to be published as a job advertisement without checking that it has not described the role in terms that would exclude protected groups under the Equality Act 2010. If a communication will be seen by a client in financial services or healthcare, apply an additional accuracy check given the regulated nature of those sectors.

When to Stop and Escalate to a Person

There are specific circumstances in which you must stop using an AI tool and refer the matter to your line manager or, where stated, to Marchwood Talent's designated data protection contact.

Escalate immediately if: a candidate or client asks how an AI system reached a decision about them — this is an Article 22 data subject right and must be handled formally; a candidate complains that an ATS outcome was discriminatory — this is both a UK GDPR complaint and a potential Equality Act 2010 matter, and under the Data (Use and Access) Act 2025 (in force from 19 June 2026 for complaints procedures) you are required to operate a complaints procedure with set response times; you discover that a colleague has been using an unapproved AI tool with candidate data; an AI output contains information you cannot verify and the communication is time-sensitive; the ATS or CRM produces a recommendation that appears to disadvantage candidates sharing a protected characteristic; or a candidate's special category data (health declaration, criminal record disclosure) has been included in an AI prompt, whether deliberately or in error.

Do not attempt to resolve any of the above situations yourself. Document what happened, preserve any relevant output or prompt text, and hand the matter to your manager before taking further action. The 72-hour breach notification window under UK GDPR Article 33 means that delay in escalating a potential data incident can itself become a compliance failure.

Special Category and Criminal Offence Data — Heightened Rules

Because Marchwood Talent places candidates into healthcare and financial services, candidate records routinely include health declarations and criminal record disclosures. Health data is special category data under UK GDPR Article 9. Criminal record data is subject to Article 10. Both categories attract stricter rules than ordinary personal data, and both are categories that the ICO regards as high-risk.

Do: Ensure that health and criminal record fields are excluded from any AI prompt or AI-processed data set unless you have confirmed in writing with your manager that there is a lawful basis under Article 9(2) or Article 10 for that processing, and that the approved AI tool has been assessed as suitable for processing that category. When using the ATS, check whether the system is configured to exclude or mask these fields from its ranking algorithm — if it is not, escalate this to your manager as a priority action because automated processing of Article 9 data without explicit consent or another Article 9(2) condition is unlawful.

Do not: Paste a CV containing a health declaration or criminal record disclosure into ChatGPT under any circumstances, even the approved enterprise account, without first confirming that the data processing agreement with OpenAI covers Article 9 and Article 10 data and that Marchwood Talent has an appropriate lawful basis for that specific processing. If in doubt, redact those fields entirely before any AI interaction.

Acknowledgement

These guidelines take effect from the date of issue: 11 August 2026. Every Marchwood Talent employee who uses any AI tool as part of their role is required to read these guidelines and confirm that they have done so. Confirmation must be recorded in the HR system. These guidelines will be reviewed when there is a material change to the tools in use, a relevant regulatory update, or in any event no later than 11 August 2027.

Questions about these guidelines should be directed to your line manager in the first instance. Data protection queries, incident reports, and candidate rights requests must be directed to Marchwood Talent's designated data protection contact.

ICO Framework Self-Assessment

The regulator's own framework, worked through and answered.

ICO AI Auditing Framework Self-Assessment — Marchwood Talent

Completed: 11 August 2026. This self-assessment works through the ICO's AI Auditing Framework against Marchwood Talent's declared AI tools (ATS automated ranking/shortlisting, ChatGPT/OpenAI, Microsoft 365 Copilot, AI-powered CRM/sales tools, AI in HR/recruitment systems) and its declared uses (candidate ranking, CV summarisation, marketing content, data analysis). Marchwood Talent places into financial services and healthcare; candidate data includes health declarations and criminal record information — both special category or sensitive data under UK GDPR. The Data (Use and Access) Act 2025 Part 5 data protection provisions came into force 5 February 2026; the complaints-procedure duty came into force 19 June 2026. Both apply now. Overall posture: HIGH RISK. No policy exists, no approved-tools register exists, and automated decisions about candidates are being made without the safeguards required by UK GDPR Art 22 or the Act.

Area 1 — Accountability and Governance

Framework question: Does the organisation have clear ownership, policies, and oversight structures for its AI systems? Rating: RED — No policy, no register of approved tools, no named AI owner, no audit trail of ATS logic or ChatGPT use.

- ☐ **Appoint a named AI Governance Lead with written terms of reference covering all AI tools in scope.**
Board or senior management formally designates one individual (or the existing DPO if one is appointed) as AI Governance Lead. Draft a one-page terms of reference covering tool approval, incident escalation, and quarterly review. Minute the appointment.
Why it matters: UK GDPR Art 5(2) accountability principle requires Marchwood Talent to demonstrate compliance; without a named owner there is no one to demonstrate it.
- ☐ **Create and maintain a live AI Tools Register listing every approved tool, its purpose, data inputs, vendor, and legal basis.**
Start with the four declared tools. For each, record: tool name, vendor, data processed, lawful basis, whether it makes or influences decisions about people, and approval date. Gate any new tool behind a sign-off step by the AI Governance Lead before first use.
Why it matters: Without a register, shadow AI use cannot be controlled and the ICO cannot see that Marchwood Talent knows what systems it operates — a core accountability failure.
- ☐ **Conduct and document a Data Protection Impact Assessment (DPIA) for the ATS automated ranking/shortlisting system before next use.**
Use the ICO's DPIA template. Map every data input to the ATS (CV fields, application form answers, criminal record and health declarations), document the automated logic if the vendor will disclose it, assess bias risk, and record residual risks and mitigations. Sign off at senior level.
Why it matters: UK GDPR Art 35 mandates a DPIA where processing is likely to result in high risk, and automated ranking of candidates using sensitive data meets that threshold; operating without one is a regulatory breach today.

Area 2 — Fair and Lawful Processing

Framework question: Is personal data processed through AI tools on a valid lawful basis, and is processing fair and non-discriminatory? Rating: RED — No documented lawful bases for any AI processing; ATS automated shortlisting is an Art 22 solely automated decision with legal/significant effect and no compliant safeguard in place; special category data (health, criminal records) processed via ChatGPT with no explicit consent or Schedule 1 condition identified.

- ☐ **Establish and document the lawful basis for each AI processing activity, including a specific condition for special category data.**

For ATS processing of standard CV data, document legitimate interests or contract performance (Art 6(1)(b) or (f)). For health declarations and criminal record data fed into any AI tool, identify an Art 9(2) condition and a Schedule 1 DPA 2018 condition — most likely explicit consent (Art 9(2)(a)) or substantial public interest with a policy document. Record each basis in the AI Tools Register.

Why it matters: Processing special category data without an Art 9(2) condition is unlawful under UK GDPR and exposes Marchwood Talent to fines up to £17.5m or 4% of global annual turnover, whichever is higher.

- ☐ **Stop pasting candidate CVs containing health or criminal record data into ChatGPT until a lawful basis, vendor data processing agreement, and transfer safeguard are confirmed.**

Issue an immediate written instruction to all consultants prohibiting this practice pending policy sign-off. Simultaneously, review OpenAI's Data Processing Addendum to confirm whether a UK-compliant DPA is in place and whether data is used to train models. Reintroduce only once these are resolved.

Why it matters: Sending special category data to a third-party AI with no DPA in place breaches UK GDPR Art 28 and Art 9 simultaneously and could constitute a personal data breach requiring ICO notification.

- ☐ **Comply with UK GDPR Art 22 and the Data (Use and Access) Act 2025 for the ATS automated shortlisting by implementing one of the three permitted safeguards.**

The ATS ranks and shortlists candidates automatically before any consultant sees them — this is a solely automated decision with significant effect on candidates. Under Art 22 and the Act (in force 5 February 2026), Marchwood Talent must either: (a) obtain explicit consent; (b) show the decision is necessary for contract; or (c) rely on authorised UK law — and in all cases must provide the right to human review, the right to contest, and the right to an explanation. Update the application process to obtain explicit consent or restructure so a consultant meaningfully reviews every candidate before shortlisting is finalised.

Why it matters: Operating an Art 22 automated decision without a compliant safeguard is an ongoing breach; the ICO's November 2024 recruitment AI audit outcomes specifically flagged this pattern in the sector.

- ☐ **Audit the ATS ranking algorithm for bias against protected characteristics under the Equality Act 2010.**

Request from the ATS vendor full documentation of the ranking criteria and training data. Run an equality impact assessment across outputs by gender, ethnicity, age, and disability. If the vendor cannot provide this, treat the system as high-risk pending replacement or manual override. Document findings and any corrective steps.

Why it matters: Placing into financial services and healthcare means any discriminatory shortlist has direct employment consequences; unlawful discrimination via an automated tool attracts employment tribunal liability as well as ICO scrutiny.

Area 3 — Transparency

Framework question: Are individuals informed, in a clear and accessible way, that AI is used to process their data and make or influence decisions about them? Rating: RED — No privacy notice references AI tools; candidates are not told the ATS ranks them automatically; no explanation of logic or right to contest is provided.

- ☐ **Update the candidate-facing privacy notice to disclose AI use, automated decision-making, and the data inputs involved.**

Add a dedicated AI section to the privacy notice covering: which tools process candidate data (ATS, and summarisation tools where used); what the ATS does (automatic ranking and shortlisting); the lawful basis; the categories of data processed; and the candidate's rights including the right to request human review and to contest the outcome. Publish this notice at the point of application, not just on the website footer.

Why it matters: UK GDPR Arts 13 and 14 require disclosure of automated decision-making logic and its consequences at the time data is collected; non-disclosure is an independent breach regardless of whether the decision itself is lawful.

- ☐ **Create a candidate-facing one-page 'How We Use AI' explainer for use in financial services and healthcare placements.**

Write a plain-English summary explaining that an ATS ranks applications, what factors it considers, that a consultant reviews shortlisted candidates, and how to request human review or raise a concern. Include the complaints procedure contact and timescales required under the Data (Use and Access) Act 2025 (duty in force 19 June 2026).

Why it matters: Healthcare and financial services candidates may submit criminal record and health data; higher-stakes placements demand a higher standard of transparency to maintain trust and meet the ICO's expectations for high-risk AI.

Area 4 — Security

Framework question: Are AI systems and the personal data they process secured appropriately, and are third-party AI vendors subject to adequate contractual controls? Rating: AMBER/RED — No DPA confirmed with OpenAI for ChatGPT use; no evidence of vendor security assessments; special category data being sent to external AI tools without documented safeguards.

- ☐ **Execute a UK GDPR-compliant Data Processing Agreement with every AI vendor that receives personal data.**

For OpenAI (ChatGPT), Microsoft (M365 Copilot), the ATS provider, and the CRM vendor: obtain or execute a written DPA containing the Art 28(3) mandatory clauses — purpose limitation, confidentiality, sub-processor controls, deletion/return obligations, and audit rights. Check each vendor's standard DPA for training-data opt-out provisions and enable them where available.

Why it matters: Art 28 UK GDPR makes Marchwood Talent liable as controller for any processing its processors carry out without a compliant DPA; the ICO can fine for the absence of the contract itself.

- ☐ **Assess and document the international transfer mechanism for any AI vendor processing data outside the UK.**

Identify where each vendor's servers are located. For transfers to the US or other non-adequate countries, confirm whether the vendor relies on the UK International Data Transfer Agreement or UK Addendum to the EU SCCs. Record the transfer mechanism in the AI Tools Register. If no adequate mechanism exists, suspend the transfer.

Why it matters: Sending candidate health and criminal record data to a US-based AI vendor without a valid transfer mechanism is an Art 46 breach and a named ICO enforcement priority.

- ☐ **Implement a Shadow AI Policy prohibiting use of non-approved AI tools with personal data, with a clear approved-tools list.**

Draft a one-page Shadow AI Policy stating: only tools on the AI Tools Register may be used with candidate or client personal data; personal data must not be pasted into any consumer AI tool not on the register; breaches are treated as a data protection incident. Circulate to all staff, obtain signed acknowledgement, and enforce via HR policy.

Why it matters: Consultants are currently pasting CVs into ChatGPT without any oversight; if a single instance involves special category data and no DPA, it is a notifiable breach — and the ICO's audit of recruitment AI specifically called out uncontrolled tool use.

Area 5 — Rights of Individuals

Framework question: Can Marchwood Talent fulfil data subject rights — access, erasure, portability, objection, and rights related to automated decisions — in relation to AI-processed data? Rating: RED — No process exists to handle Art 22 contests; no documented procedure for subject access requests that include AI-derived outputs; no complaints procedure meeting the Data (Use and Access) Act 2025 duty.

☐ **Build and document a procedure for candidates to request human review of any automated ATS shortlisting decision.**

Designate a named contact for human review requests. Set a response timescale (recommend five working days). Confirm that a consultant will re-evaluate the application independently of the ATS ranking. Log every request and outcome. Reference this procedure in the privacy notice and the candidate AI explainer.

Why it matters: UK GDPR Art 22(3) and the Data (Use and Access) Act 2025 require the right to obtain human intervention, express a point of view, and contest the decision; failure to provide this mechanism is an enforceable breach.

☐ **Establish a complaints procedure meeting the Data (Use and Access) Act 2025 duty (in force 19 June 2026) with defined response timescales.**

Draft a written complaints procedure covering: how to submit a data protection or AI-related complaint, who handles it, and the maximum response period. Publish this procedure on the Marchwood Talent website and in candidate-facing materials. Log all complaints and outcomes.

Why it matters: The duty to operate a complaints procedure and respond within set timescales has been in force since 19 June 2026; Marchwood Talent is already out of compliance on this point and it is a straightforward fix.

☐ **Update the Subject Access Request procedure to include retrieval of AI-generated outputs (ATS scores, rankings, CV summaries) held against a candidate's record.**

Map where ATS rank scores, shortlisting flags, and any ChatGPT-generated summaries are stored. Ensure the SAR response process retrieves these alongside standard application data. Where AI outputs are stored in CRM or ATS, confirm the system can export them in a readable format within the statutory one-month period.

Why it matters: AI-derived scores and summaries are personal data; omitting them from an SAR response is an Art 15 breach and — given healthcare and financial services placements — is likely to prompt escalation to the ICO.

Lowest-Scoring Areas — Priority Action Summary

Three areas score RED and require immediate action before any further AI-assisted candidate processing takes place. The following items are the highest-priority outputs of this self-assessment, ranked by risk to Marchwood Talent.

☐ **Suspend ChatGPT use for CV processing involving health or criminal record data immediately and do not reinstate until a DPA, transfer mechanism, and lawful basis are in place.**

Issue a written all-staff instruction today. Simultaneously instruct the AI Governance Lead to complete vendor due diligence on OpenAI within 10 working days. Document the suspension decision and the reinstatement criteria.

Why it matters: This is the single highest-risk activity: special category data sent to an external AI with no contract, no transfer safeguard, and no lawful basis — all three are independent UK GDPR breaches, each carrying fines up to £17.5m or 4% of global annual turnover.

☐ **Commission a DPIA for the ATS and implement Art 22 safeguards before the next automated shortlisting cycle.**

Engage the ATS vendor this week to obtain algorithm documentation. Complete the DPIA using the ICO template within 20 working days. Implement explicit consent capture or human review sign-off before any candidate is excluded from consideration by the ATS alone.

Why it matters: The ICO published recruitment AI audit outcomes in November 2024 specifically addressing automated shortlisting; Marchwood Talent's current practice is the fact pattern those outcomes warned against, and enforcement risk is material.

☐ **Draft and publish the Shadow AI Policy and AI Tools Register within 15 working days and train all consultants on both.**

Use the AI Tools Register structure described in Area 1. Circulate the Shadow AI Policy to all 11–50 employees with a mandatory read-and-sign step. Deliver a 30-minute briefing session covering what is permitted, what is not, and how to raise concerns.

Why it matters: Without a policy and register, every consultant's AI use is ungoverned; Marchwood Talent cannot demonstrate accountability to the ICO, an insurer, or a financial services or healthcare client conducting due diligence.

Compliance Roadmap

The sequence to work through. Do not start a phase until the one before it is complete — the order is deliberate.

Phase 1 — Immediate Actions (Days 1–14)

These actions must be completed before any other phase begins. Marchwood Talent is currently operating AI tools that process special category data — health declarations and criminal record information — without a policy, an approved-tools register, or documented safeguards. That combination creates live regulatory exposure under UK GDPR and the Equality Act 2010 today. Complete every item in this phase before moving to Phase 2.

- ☐ **Issue an immediate instruction to all consultants prohibiting the pasting of candidate CVs or any personal data into ChatGPT or any other unapproved external AI tool.**

The Managing Director or Head of Operations sends a written all-staff notice — email is sufficient at this stage — stating that pasting candidate data into ChatGPT, or any tool not yet formally approved by the business, is suspended with immediate effect pending a policy review. The notice must name ChatGPT specifically and make clear it covers CV text, cover letters, application forms, health declarations, and criminal record disclosures. Acknowledge receipt from each employee in writing.

Why it matters: Every CV pasted into ChatGPT is a transfer of personal data to OpenAI's infrastructure without a documented lawful basis, a data processing agreement, or any assessment of cross-border transfer risk — a breach of UK GDPR Articles 5, 6, and 28 that the ICO could act on immediately if a complaint were filed.

- ☐ **Convene an emergency senior meeting and appoint a named AI Compliance Owner for Marchwood Talent.**

Hold a one-hour meeting of directors and any senior operations or HR lead. Formally record in the meeting minutes that a named individual — a director if no other qualified person exists — is accountable for AI compliance. That person owns the roadmap, signs off each deliverable, and is the single point of contact if the ICO makes contact. Record the appointment in writing.

Why it matters: Without a named owner, this roadmap will stall; the ICO expects a responsible person to be identifiable, and the absence of accountability is an aggravating factor in any enforcement assessment.

- ☐ **Compile an emergency inventory of every AI tool currently in use across Marchwood Talent, including tools used without prior approval.**

The AI Compliance Owner sends a short written survey to all staff asking them to list every AI tool, plugin, or automated feature they use in their work — including free-tier tools, browser extensions, and anything built into existing software such as Microsoft 365 Copilot or the ATS. Collate responses within five working days. Record tool name, vendor, what data is entered, and who uses it. This is the Shadow AI audit.

Why it matters: Marchwood Talent has no record of which tools are approved; without this inventory, it is impossible to assess which processing activities are lawful, which require a Data Protection Impact Assessment, or which must be suspended.

Phase 2 — Foundational Documentation (Weeks 2–6)

Once the immediate suspension is in place and the inventory is complete, Marchwood Talent must build the documentary foundation that UK GDPR, the Data (Use and Access) Act, and the ICO AI Auditing Framework all require before AI tools can be reintroduced to live use. No AI tool should be reinstated until the item governing it in this phase is complete.

☐ **Conduct a Data Protection Impact Assessment for the ATS automated ranking and shortlisting function.**

Using the ICO's published DPIA template, document: the purpose of the automated ranking, the data inputs (including any fields that correlate with protected characteristics such as name, address, or education history), the logic applied by the ATS vendor, the risks of discriminatory outputs, and the measures Marchwood Talent will take to mitigate those risks. Contact the ATS vendor in writing to obtain a description of the algorithm and its training data. The DPIA must be completed and signed off by the AI Compliance Owner before the shortlisting feature is used again. Retain the document.

Why it matters: Automated candidate ranking is processing that is likely to result in significant effects on individuals; a DPIA is mandatory under UK GDPR Article 35, and operating without one while processing special category data exposes Marchwood Talent to fines up to £17.5 million or 4% of global annual turnover, whichever is higher.

☐ **Determine and document the lawful basis and, where required, the explicit condition for processing special category data through AI tools.**

For health declarations and criminal record data processed through the ATS or any other AI tool, identify the Article 9 condition (most likely explicit consent or the employment-related Schedule 1 condition under the Data Protection Act 2018) and, for criminal record data, the Article 10 condition. Document these in the Record of Processing Activities. Where explicit consent is relied upon, create or update the candidate consent form to be specific about AI processing.

Why it matters: Processing special category data without a valid Article 9 condition is unlawful regardless of any other safeguard; a single candidate complaint to the ICO concerning health or criminal record data in the ATS would be very likely to trigger a formal investigation.

☐ **Draft and adopt an AI Acceptable Use Policy covering all tools identified in the Phase 1 inventory.**

The policy must list every approved tool with its permitted use, the data that may and may not be entered, the prohibition on entering special category data into tools without a completed DPIA, the requirement for human review of any AI output before it affects a candidate, and the process for requesting approval of a new tool. Circulate to all staff, obtain signed acknowledgement, and version-control the document. Review it whenever a new tool is adopted.

Why it matters: The ICO's audit of AI tools in recruitment, published November 2024, identified the absence of an acceptable use policy as a primary governance gap; without it, Marchwood Talent cannot demonstrate to a regulator, insurer, or client that its AI use is controlled.

☐ **Review and update all candidate-facing privacy notices to disclose AI processing, automated decision-making, and candidates' rights.**

Amend the candidate privacy notice to state: which AI tools process their data, that automated ranking occurs in the ATS before consultant review, what logic is applied at a high level, that no purely automated decision is taken without human review (or, if one is, their rights under UK GDPR Article 22 and the Data (Use and Access) Act), and how to request human intervention or object. Publish the updated notice on the Marchwood Talent website and include it in all new candidate registration communications.

Why it matters: UK GDPR Articles 13 and 14 require disclosure of automated processing at the point of data collection; failure to disclose is a standalone breach and would compound any enforcement action relating to the ATS.

☐ **Establish or update the Article 30 Record of Processing Activities to include all AI-assisted processing.**

Add a dedicated AI processing section to the existing ROPA (or create one if none exists). For each AI tool, record: the tool and vendor, the categories of data processed, the purpose, the retention period, the lawful basis, any transfers outside the UK, and the safeguards in place. This document is a live record — update it each time a tool is added or removed. The AI Compliance Owner is responsible for maintaining it.

Why it matters: The ICO can request the ROPA at any time; an absent or incomplete record is itself a breach of UK GDPR Article 30 and signals to the regulator that broader governance failures are likely.

☐ **Execute or verify Data Processing Agreements with every AI vendor whose tools are approved for use.**

Identify the relevant vendor contracts for the ATS, Microsoft 365 Copilot, and any approved CRM. Confirm a UK GDPR-compliant DPA (Article 28) is in place with each, covering instruction-based processing, security obligations, sub-processor disclosure, and data deletion on termination. Where OpenAI is concerned, note that its terms must be reviewed against UK GDPR Article 28 requirements; if ChatGPT is to be re-approved, the enterprise or API tier with a DPA is required — the consumer tier is not compliant for this purpose.

Why it matters: Processing candidate data through a vendor without a compliant DPA makes Marchwood Talent jointly liable for the vendor's processing failures and removes any contractual route to enforce data deletion or breach notification obligations.

Phase 3 — Bias, Equality, and Human Oversight Controls (Weeks 4–10)

Phases 1 and 2 address the legal paperwork. Phase 3 addresses the operational risk of discriminatory outcomes from the ATS ranking system and any other AI tool that influences decisions about candidates. This phase may run concurrently with Phase 2 from week 4, but must be fully complete before the ATS shortlisting function is returned to live production use.

☐ **Obtain and review the ATS vendor's bias testing documentation and equal opportunities impact data for the ranking algorithm.**

Write to the ATS vendor requesting: the protected characteristics considered during algorithm design and testing, any disparate impact testing carried out, the training data used, and any known limitations. If the vendor cannot provide this, escalate in writing and consider whether continued use of the automated ranking feature is defensible. Document the vendor's response or non-response. Compare the algorithm's documented logic against the protected characteristics listed in the Equality Act 2010.

Why it matters: If the ATS ranking algorithm produces systematically lower scores for candidates with characteristics protected under the Equality Act 2010 — including age, race, sex, or disability — Marchwood Talent is exposed to indirect discrimination claims and potential ICO action; ignorance of the algorithm is not a defence.

☐ **Implement and document a mandatory human review stage that occurs before any ATS-generated shortlist is shared with a client or acted upon.**

Create a written procedure — one page is sufficient — requiring a named consultant to review every ATS shortlist before it is sent to a client, checking for obvious demographic imbalance, unexplained exclusions, and whether the ranking appears consistent with the role criteria. The consultant records their review in the ATS or a simple log with date, role, and sign-off. This procedure must be included in the AI Acceptable Use Policy.

Why it matters: UK GDPR Article 22 and the Data (Use and Access) Act together require meaningful human involvement in decisions that significantly affect individuals; a shortlist handed to a financial services or healthcare client without human review may constitute an unlawful solely automated decision, triggering individual rights and regulatory liability.

☐ **Run bias monitoring on the ATS output for the first three months after reintroduction, comparing shortlisted versus rejected candidate profiles by observable demographic proxies.**

Using anonymised data from the ATS, compare the proportion of shortlisted candidates by gender, age band, and where data is held, ethnicity, against the full applicant pool for at least three consecutive months. Record the results in a simple spreadsheet. If a statistically notable disparity appears for any group, suspend the automated ranking and notify the AI Compliance Owner. Document the methodology and outputs.

Why it matters: The ICO AI Auditing Framework explicitly requires ongoing bias monitoring for AI systems used in employment decisions; without it, Marchwood Talent cannot demonstrate compliance to the ICO or defend against an Equality Act 2010 indirect discrimination claim.

- ☐ **Establish a documented process for candidates to request human review of any AI-influenced decision and to receive a meaningful explanation.**

Add a specific contact route — an email address is sufficient — to the candidate privacy notice and to any rejection communication, stating that candidates may request human review of any decision and an explanation of the factors considered. Assign a responsible person to handle these requests. Document each request and the response.

Responses to data protection complaints must now be provided within the timeframes set by the Data (Use and Access) Act, which brought the complaints procedure duty into force on 19 June 2026.

Why it matters: The duty on controllers to operate a complaints procedure and respond within set timeframes has been in force since 19 June 2026; failing to have this route in place means Marchwood Talent is already in breach of a live statutory obligation.

Phase 4 — Shadow AI and Tool Approval Governance (Weeks 6–12)

The Phase 1 inventory will have revealed tools being used without approval. This phase formalises the process that prevents that situation recurring and creates the governance structure for evaluating any new AI tool before it touches candidate data.

- ☐ **Categorise every tool from the Phase 1 inventory as Approved, Approved with Restrictions, or Suspended pending DPIA.**

The AI Compliance Owner reviews each tool against three criteria: is a compliant DPA in place, has a DPIA been completed where required, and does the tool's data handling meet UK GDPR standards. Record the categorisation in a simple AI Tools Register with the date of assessment, the outcome, and any conditions. Communicate the register to all staff and confirm that Suspended tools may not be used until the conditions are met.

Why it matters: Without a formal approved list, the Shadow AI problem identified in Marchwood Talent's own concerns will continue; the next consultant to paste a health declaration into an unapproved tool creates a fresh breach that the business cannot mitigate after the fact.

- ☐ **Create a one-page New Tool Request procedure that any member of staff must complete before adopting an AI tool.**

The procedure requires the requesting employee to state the tool name, intended use, data to be entered, and vendor details. The AI Compliance Owner then checks for a DPA, assesses whether a DPIA is needed, and records approval or refusal within ten working days. No tool is used until written approval is recorded. The procedure and the AI Tools Register are maintained by the AI Compliance Owner and reviewed quarterly.

Why it matters: A structured approval gate is the only reliable control against Shadow AI; its absence means Marchwood Talent cannot demonstrate to the ICO that it has taken reasonable steps to prevent unauthorised processing, which weakens its position in any enforcement or audit scenario.

- ☐ **Deliver a one-hour AI compliance briefing to all staff, covering the Acceptable Use Policy, the approved tools list, and the consequences of non-compliance.**

The AI Compliance Owner or an external facilitator delivers the session — in person or by video call — covering: what the business's AI tools do, what data must never be entered into any AI tool without explicit approval, how to request a new tool, and what happens if the policy is breached. Record attendance. Repeat for any new joiner within their first two weeks. Document completion in the staff training log.

Why it matters: Staff who do not know the rules cannot follow them; the ICO considers staff training a basic accountability measure, and its absence is a factor that increases the likelihood of an enforcement outcome if a breach occurs.

Phase 5 — Sector-Specific and Regulatory Obligations (Weeks 8–16)

Marchwood Talent places candidates into financial services and healthcare — two of the most scrutinised sectors in the UK. The FCA and MHRA apply AI principles within their domains, and clients in those sectors will increasingly require evidence of Marchwood Talent's own AI governance as part of their supplier due diligence. This phase addresses those obligations.

- ☐ **Review all standard client contracts with financial services and healthcare clients to confirm that Marchwood Talent's AI use disclosures meet those clients' own regulatory obligations.**

For each active financial services and healthcare client, check whether the client contract or supplier code requires disclosure of AI use in the recruitment process. Where it does, provide written confirmation of the AI tools used, the safeguards in place, and the human review process. Where the contract is silent, add a standard AI disclosure clause to the next contract renewal. Retain copies of all disclosures.

Why it matters: An FCA-regulated client that discovers Marchwood Talent processed candidate health or criminal record data through an unapproved AI tool without disclosure may terminate the contract and report the matter to the ICO; proactive disclosure protects the commercial relationship and demonstrates accountability.

- ☐ **Confirm the legal basis and specific safeguards for processing criminal record data through the ATS, given the placements into financial services and healthcare.**

Criminal record data is subject to UK GDPR Article 10 and requires either official authority or a specific Data Protection Act 2018 Schedule 1 condition. Confirm in writing with your DPA adviser which condition applies to Marchwood Talent's processing, document it in the ROPA, and ensure the ATS is configured so that criminal record fields are not automatically weighted in the ranking algorithm without explicit justification recorded for each role.

Why it matters: Automated weighting of criminal record data in a ranking algorithm, without a documented Schedule 1 condition, is unlawful processing of Article 10 data and would be treated as a serious breach by the ICO, particularly given the volume of candidates placed into regulated sectors.

- ☐ **Assess Microsoft 365 Copilot's configuration to confirm that candidate data held in email, Teams, or SharePoint is not being used to train or inform Copilot outputs shared beyond the intended recipients.**

Contact Marchwood Talent's Microsoft 365 administrator or Microsoft directly and confirm the tenant configuration settings for Copilot data use. Ensure that the Microsoft data processing terms are activated for the business's subscription tier, that Copilot is not configured to surface data across organisational boundaries, and that any AI-generated summaries of candidate communications are treated as personal data in their own right. Document the configuration settings and the date of review.

Why it matters: Microsoft 365 Copilot operates across the full data estate; without verified configuration, candidate health or financial data in emails could be surfaced to unintended users, constituting a personal data breach under UK GDPR Article 33 requiring notification to the ICO within 72 hours.

Phase 6 — Foundational Compliance Declaration and Ongoing Monitoring

Marchwood Talent can honestly state that it has foundational compliance in place when every item in Phases 1 through 5 is documented and evidenced. That point is realistically achievable within 16 weeks of starting this roadmap, assuming the Phase 1 suspension is enacted on day one. Ongoing monitoring is not optional — it is the mechanism by which compliance remains real rather than becoming a paper exercise.

- ☐ **Complete a Foundational Compliance Checklist and file it as a dated, signed record in the AI compliance folder.**

The AI Compliance Owner produces a single document listing each deliverable from Phases 1 to 5, confirms in writing that each is complete with a reference to the supporting document, and signs and dates it. The Managing Director countersigns. This document is the evidence base if the ICO, an insurer, or a client asks whether Marchwood Talent has an AI compliance programme. It is updated at each subsequent quarterly review.

Why it matters: UK GDPR Article 5(2) requires controllers to demonstrate compliance, not merely achieve it; a signed checklist backed by the underlying documents is the minimum evidence needed to discharge the accountability principle in an ICO inquiry.

☐ **Schedule quarterly reviews of the AI Tools Register, the Acceptable Use Policy, and the bias monitoring outputs.**

The AI Compliance Owner books a recurring quarterly meeting — 90 minutes — to review: any new tools adopted or requested, any bias monitoring findings from the ATS, any candidate complaints received and how they were resolved, any relevant ICO or FCA guidance published in the preceding quarter, and any changes to the tools' terms of service that affect data processing. Update the ROPA and DPIA where the review identifies a material change.

Why it matters: AI tools and the regulatory landscape governing them change rapidly — the ICO published its recruitment AI audit outcomes in November 2024 and the Data (Use and Access) Act commenced in February 2026; a compliance programme that is not reviewed will become outdated and cease to be a defence.

☐ **Subscribe to ICO enforcement updates and FCA AI-related guidance, and assign responsibility for reviewing them to the AI Compliance Owner.**

Register for the ICO's email updates at ico.org.uk and the FCA's newsletter. When a relevant enforcement decision, audit outcome, or guidance document is published, the AI Compliance Owner reads it within ten working days and records whether any action is required for Marchwood Talent. Material changes are escalated to the board within 30 days.

Why it matters: The UK regulatory environment for AI is explicitly evolving — the AI Minister signalled in August 2026 that statutory rules for advanced AI models are under consideration; businesses that monitor developments can adapt before a new obligation becomes enforceable, rather than after a breach has occurred.

☐ **Conduct an annual internal AI audit against the ICO AI Auditing Framework and update the DPIA for the ATS.**

Each year, using the ICO's published AI Auditing Framework as the assessment structure, review Marchwood Talent's AI tools against the framework's accountability, transparency, fairness, and security dimensions. Produce a short written report of findings and any remedial actions. Update the ATS DPIA to reflect any changes in the algorithm, the data processed, or the candidate population. File the report alongside the Foundational Compliance Checklist.

Why it matters: The ICO conducted a recruitment AI audit in November 2024 and has named AI in employment decisions as a priority area; an annual internal audit demonstrates proactive accountability and substantially reduces the risk of adverse findings in any external ICO audit of Marchwood Talent.

Data Classification Matrix

Which categories of your data may go near an AI tool, and which may never. The one page staff refer to before pasting anything in.

Classification	Examples in this business	May be used with AI?	Conditions for permitted use	Approval required from
PUBLIC	Marchwood Talent website copy, published job adverts, sector salary guides shared externally, approved social media posts	YES — all approved tools	Use only approved tools (ChatGPT, M365 Copilot, ATS, CRM). No conditions beyond standard tool-use policy.	None — self-service permitted
INTERNAL	Internal process guides, consultant KPI dashboards, anonymised placement volume reports, generic email templates, CRM pipeline summaries with no named individuals	YES — approved tools only	Data must be genuinely anonymised before input. Do not paste named client or candidate fields. M365 Copilot preferred as data stays within tenancy.	Line manager if uncertain whether data is truly anonymised
CONFIDENTIAL	Named candidate CVs, contact details, employment history, salary expectations, client vacancy briefs, consultant performance records, named client account data	RESTRICTED — see conditions	M365 Copilot only (data stays in tenancy). ChatGPT and external AI tools are PROHIBITED for named personal data. ATS automated ranking requires a DPIA and human review before any shortlist is acted on. UK GDPR Art 5(1)(f) and Art 32 apply.	Senior consultant or line manager before processing; Data Protection Lead for any new use case
SPECIAL CATEGORY — Health	Candidate health declarations (mandatory in healthcare placements), disability disclosures, reasonable adjustment requests, occupational health information	NO — prohibited in external AI tools	NEVER paste into ChatGPT or any external AI tool. M365 Copilot use requires explicit consent (UK GDPR Art 9(2)(a)) or legal claim basis (Art 9(2)(f)) plus a completed DPIA. ATS must not score or rank on health data; any such field must be excluded from automated ranking logic.	Data Protection Lead and, where applicable, legal adviser — prior written sign-off required
SPECIAL CATEGORY — Criminal Offence Data	DBS check results, criminal record declarations required for financial services (FCA fit-and-proper) and healthcare placements, cautions or convictions disclosed by candidates	NO — prohibited in all AI tools	NEVER input into any AI tool including M365 Copilot, ChatGPT, ATS ranking modules, or CRM. Processed only by authorised personnel under Schedule 1 DPA 2018 condition. Stored in access-controlled system only. UK GDPR Art 10 and DPA 2018 s.10 apply.	Data Protection Lead only — no delegation permitted
RESTRICTED	Aggregated financial performance data, merger or acquisition information, regulator correspondence, legal advice, ATS vendor contracts containing data processing terms	NO	Restricted data is not to be processed by any AI tool. These records are commercially or legally sensitive and are outside the scope of any current AI use case at Marchwood Talent.	Director-level authorisation required before any change to this prohibition

DOCUMENT: Data Classification Matrix | OWNER: Data Protection Lead | VERSION DATE: 11 August 2026 | REVIEW
CADENCE: Every 12 months or on adoption of any new AI tool, whichever is sooner.

APPROVED AI TOOLS (as at 11 August 2026): ChatGPT / OpenAI; Microsoft 365 Copilot; the incumbent ATS with automated candidate ranking; AI-powered CRM. Any tool not on this list is unauthorised. Consultants must not use unauthorised tools ('shadow AI') for any business data — see Marchwood Talent Shadow AI Policy.

AUTOMATED DECISION-MAKING (ATS RANKING): The ATS ranks and shortlists candidates without consultant review. This constitutes solely automated decision-making with legal or similarly significant effect under UK GDPR Art 22. Under the Data (Use and Access) Act 2025 (most Part 5 provisions in force 5 February 2026), wider lawful bases are available but the associated safeguards are mandatory, including the right to human review and the right to contest. A DPIA covering the ATS ranking logic is required before any shortlist is used in a placement decision. A qualified consultant must review every ranked shortlist before it is shared with a client or acted upon.

COMPLAINTS PROCEDURE: From 19 June 2026, Marchwood Talent is under a statutory duty (Data (Use and Access) Act 2025) to operate a complaints procedure and respond to data protection complaints within set time limits. The Data Protection Lead is responsible for maintaining and publicising this procedure.

BIAS AND EQUALITY: The ATS ranking algorithm must be audited against the ICO AI Auditing Framework to identify and mitigate bias risks. Proxy discrimination — where a ranking factor correlates with a protected characteristic — may constitute unlawful indirect discrimination under the Equality Act 2010. Financial services and healthcare placements involve FCA and MHRA sector expectations respectively; bias in candidate selection in these sectors carries heightened regulatory risk.

SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA — SECTOR NOTE: Marchwood Talent places candidates into healthcare and financial services roles. Candidate health declarations and DBS / criminal record data are therefore routinely collected. These are the highest-risk data types under UK GDPR. The maximum ICO fine is £17.5 million or 4% of global annual turnover — the turnover-based limb cannot be computed without Marchwood Talent's figures, but the statutory ceiling is £17.5 million. Neither health nor criminal offence data may enter any AI tool under any circumstances without prior written approval from the Data Protection Lead and satisfaction of a specific Schedule 1 DPA 2018 condition.

CHATGPT / EXTERNAL AI: When a consultant pastes a CV into ChatGPT, that personal data is transmitted to OpenAI's systems outside Marchwood Talent's control. This is an international transfer under UK GDPR Chapter V and requires a lawful transfer mechanism. For named or confidential data this practice is prohibited unless a compliant data processing agreement and transfer mechanism are in place and documented. Consultants must use M365 Copilot as the default summarisation tool for CVs containing personal data.

GDPR Compliance Position

Your documented data protection position for each AI tool — what a customer's procurement team asks for.

ATS with Automated Candidate Ranking and Shortlisting

GDPR COMPLIANCE POSITION — ATS WITH AUTOMATED CANDIDATE RANKING AND SHORTLISTING

Marchwood Talent | Prepared: 11 August 2026

CONTROLLER / PROCESSOR ROLES AND LAWFUL BASIS

Marchwood Talent is the data controller. The ATS vendor is a data processor acting on Marchwood's documented instructions. The ATS performs automated ranking and shortlisting of candidates before any consultant review. This constitutes solely automated decision-making that produces a significant effect on candidates (exclusion from consideration for roles). UK GDPR Article 22(1) therefore applies and prohibits such processing unless a specific condition in Article 22(2) is met. The Data (Use and Access) Act 2025 (in force 5 February 2026) amended the lawful bases available for solely automated decisions and introduced accompanying safeguards; those provisions are now in force and Marchwood must comply with them. The lawful basis for processing ordinary candidate data is Article 6(1)(b) (performance of a contract / steps at the data subject's request) or Article 6(1)(f) (legitimate interests), to be documented in the Record of Processing Activities. For health declarations and criminal record information, a separate Article 9 and Schedule 1 DPA 2018 condition is required (see below). No Article 22 condition has been documented. This is a live compliance gap.

CATEGORIES OF DATA AND OF DATA SUBJECT

Data subjects: job applicants (candidates) placing into financial services and healthcare roles. Categories of data processed by the ATS: name, contact details, employment history, qualifications, right-to-work information, health declarations (special category data — Article 9 UK GDPR), criminal record information (Article 10 UK GDPR / Schedule 1 DPA 2018). The presence of health and criminal record data in a system performing automated ranking significantly elevates the risk profile. Processing these categories for automated decisioning without an explicit Article 9 condition (most likely Schedule 1 paragraph 18 DPA 2018 — recruitment) and a suitable policy document in place is unlawful.

TRANSFER POSITION AND MECHANISM

The transfer position depends on where the ATS vendor hosts and processes data. Marchwood has not documented this. If the vendor processes data outside the UK (including in the USA or EU), a UK-approved transfer mechanism is required under UK GDPR Chapter V — either an adequacy decision, International Data Transfer Agreement (IDTA), or UK Addendum to EU SCCs. This must be confirmed with the vendor and recorded. Until confirmed, an international transfer risk cannot be ruled out and must be treated as unmitigated.

RETENTION AND MODEL-TRAINING POSITION

Marchwood has no documented retention schedule for ATS data. UK GDPR Article 5(1)(e) (storage limitation) requires that personal data be kept no longer than necessary. A defined retention period — typically six to twelve months for unsuccessful candidates in recruitment, subject to sector-specific requirements — must be set and enforced. Marchwood must obtain written confirmation from the ATS vendor that candidate data is not used to train or improve any AI model (the vendor's own or a third party's). If the vendor's terms permit model training on client data, those terms must be renegotiated or the vendor replaced. This is unconfirmed and is a compliance gap.

WHETHER A DPA IS IN PLACE AND WHAT IS MISSING

UK GDPR Article 28 requires a written Data Processing Agreement with every processor. It is not confirmed that a compliant Article 28 DPA is in place with the ATS vendor. Required DPA content includes: subject matter and duration, nature and purpose of processing, type of personal data and categories of data subject, obligations and rights of the controller, restrictions on sub-processing, data security measures, deletion or return of data on termination, audit rights, and assistance with data subject rights requests. Marchwood must obtain and review this document immediately. If not in place, processing via the ATS is in breach of Article 28.

OVERALL POSITION FOR THIS TOOL

High risk. The ATS performs automated candidate ranking on data that includes special category and criminal record information, with no Article 22 condition documented, no Article 9 condition and suitable policy document confirmed, no verified DPA, no confirmed transfer mechanism, no retention schedule, and no model-training restriction confirmed. Immediate remediation is required before this processing can be considered lawful.

ChatGPT / OpenAI

GDPR COMPLIANCE POSITION — CHATGPT / OPENAI

Marchwood Talent | Prepared: 11 August 2026

CONTROLLER / PROCESSOR ROLES AND LAWFUL BASIS

Marchwood Talent is the data controller when its consultants paste candidate CV data into ChatGPT. OpenAI's role depends on the product and configuration: under the ChatGPT Team, Enterprise, or API arrangements, OpenAI can act as a data processor; under a standard consumer ChatGPT account, OpenAI acts as an independent controller and does not accept Article 28 DPA obligations. Marchwood's consultants are currently pasting CVs into ChatGPT without a confirmed enterprise arrangement — this means OpenAI is most likely acting as an independent controller, which means Marchwood is disclosing candidate personal data to a third party without lawful basis, without notice to the data subject, and without a DPA. The lawful basis Marchwood relies on for CV processing is Article 6(1)(b) or 6(1)(f); neither extends to disclosure to an uncontracted third party.

CATEGORIES OF DATA AND OF DATA SUBJECT

Data subjects: job candidates. Categories of data pasted into ChatGPT include: full name, contact details, employment history, qualifications, and — because Marchwood places into financial services and healthcare — potentially health declarations and criminal record information. Pasting special category data (Article 9) or criminal record data (Article 10) into a consumer AI tool with no DPA and no confirmed data boundary is among the highest-risk processing activities Marchwood undertakes. This is a current, active compliance failure.

TRANSFER POSITION AND MECHANISM

OpenAI processes data in the United States. Under a consumer or unverified arrangement, no UK-approved transfer mechanism (IDTA, adequacy decision, or UK Addendum) is in place. This means every CV pasted into ChatGPT involves an unlawful international transfer of personal data under UK GDPR Chapter V. If Marchwood moves to a confirmed ChatGPT Enterprise or API arrangement, OpenAI offers contractual terms that include an IDTA-equivalent mechanism; this must be verified and documented. Until that is confirmed, the transfer is unlawful.

RETENTION AND MODEL-TRAINING POSITION

Under standard ChatGPT accounts, OpenAI's default settings include use of conversations to improve its models. This means candidate CV data pasted by consultants may be used to train OpenAI's AI systems — a disclosure to a third party for a purpose entirely outside the scope of the candidate's consent or any lawful basis Marchwood can rely on. Under a ChatGPT Enterprise arrangement, OpenAI commits that data is not used for model training; this is the minimum acceptable configuration. Marchwood must move to an enterprise arrangement with written confirmation that no candidate data is retained beyond the session or used for training, or must prohibit use of ChatGPT for candidate data entirely.

WHETHER A DPA IS IN PLACE AND WHAT IS MISSING

No Article 28 DPA is confirmed to be in place with OpenAI for this use. Under a consumer account, none is available. This is a fundamental breach of Article 28. To remediate, Marchwood must: (1) immediately prohibit consultants from pasting candidate data into standard ChatGPT accounts; (2) procure a ChatGPT Enterprise or API arrangement that includes a compliant Article 28 DPA, transfer mechanism, model-training opt-out, and data deletion terms; and (3) issue an internal directive pending that procurement. The absence of any policy means consultants have no guidance — this is the core shadow-AI risk identified by Marchwood.

OVERALL POSITION FOR THIS TOOL

Critical risk. Current use involves unlawful disclosure of candidate personal data (including likely special category data) to an uncontracted third party, unlawful international transfer, and probable use of that data for AI model

training. This use must be suspended for candidate data immediately and only reinstated under a compliant enterprise arrangement with a verified DPA and transfer mechanism.

Microsoft 365 Copilot

GDPR COMPLIANCE POSITION — MICROSOFT 365 COPILOT

Marchwood Talent | Prepared: 11 August 2026

CONTROLLER / PROCESSOR ROLES AND LAWFUL BASIS

Marchwood Talent is the data controller. Microsoft acts as a data processor under the Microsoft Product Terms and Data Protection Addendum (DPA), which constitutes a compliant Article 28 agreement. Copilot processes data within the Microsoft 365 tenant on Marchwood's behalf. The lawful basis for processing candidate or employee data through Copilot tasks (drafting, summarising, analysing) is Article 6(1)(b) or 6(1)(f) for ordinary personal data, with the same Article 9 / Schedule 1 conditions required where health or criminal record data is involved. Marchwood must document which Copilot use cases involve personal data and which lawful basis applies to each.

CATEGORIES OF DATA AND OF DATA SUBJECT

Data subjects include candidates (where Copilot is used for recruitment tasks such as drafting job adverts, summarising applications, or generating communications) and employees (where Copilot is used in HR or performance management workflows). Categories of data potentially in scope: name, contact details, employment history, performance records, health information, criminal record information. Marchwood must ensure that Copilot's access within the Microsoft 365 environment is scoped appropriately — if candidate files containing special category data are accessible to Copilot, the Article 9 condition must cover that processing.

TRANSFER POSITION AND MECHANISM

Microsoft's EU Data Boundary and UK data residency commitments mean that for commercial Microsoft 365 subscribers, data is processed within the EU/UK region by default. Microsoft's DPA includes Standard Contractual Clauses and the UK Addendum for international transfers. The transfer position for Copilot under a standard M365 commercial licence is therefore covered, subject to Marchwood verifying its specific tenant configuration and that UK data residency is active. Marchwood should obtain written confirmation of the data residency settings from its Microsoft licensing agreement or reseller.

RETENTION AND MODEL-TRAINING POSITION

Microsoft commits under its commercial terms that Copilot does not use customer data (including prompts and outputs) to train its foundational AI models. Copilot interaction data is retained within the Microsoft 365 tenant subject to Marchwood's own retention policies. Marchwood must set and enforce retention labels within Microsoft Purview for Copilot outputs and interaction logs. Where Copilot outputs contain candidate or employee personal data, those outputs must be subject to the same retention schedule as other HR and recruitment records. This is under Marchwood's control and must be configured.

WHETHER A DPA IS IN PLACE AND WHAT IS MISSING

Microsoft's Data Protection Addendum is incorporated by reference into the Microsoft Product Terms and is available at Microsoft's Trust Centre. This constitutes a compliant Article 28 DPA, provided Marchwood is on a commercial licence (M365 Business or Enterprise). Marchwood must confirm it is not using Copilot under a personal or trial account, which may carry different terms. Subject to that confirmation, the DPA position for Copilot is the strongest of all tools in scope. Remaining gaps: (1) no documented Copilot-specific data handling policy internal to Marchwood; (2) no retention configuration confirmed; (3) no documented restriction on which data types consultants may process through Copilot.

OVERALL POSITION FOR THIS TOOL

Moderate risk, materially lower than the ATS or ChatGPT. The Microsoft DPA and model-training commitments provide a lawful processing foundation. Marchwood's gaps are internal: no usage policy, no retention configuration, and no documented restriction on processing special category data through Copilot without first confirming an Article 9 condition is in place. These are remediable through internal policy and tenant configuration.

AI in HR or Recruitment Systems

GDPR COMPLIANCE POSITION — AI IN HR OR RECRUITMENT SYSTEMS

Marchwood Talent | Prepared: 11 August 2026

CONTROLLER / PROCESSOR ROLES AND LAWFUL BASIS

This category covers AI functionality embedded in HR or recruitment platforms beyond the primary ATS (for example, AI-assisted interview scheduling, candidate scoring within an HR platform, or AI-generated performance assessments for placed contractors). Marchwood Talent is the data controller for all such processing. Platform vendors are data processors. Lawful basis for ordinary personal data is Article 6(1)(b) or 6(1)(f). Where AI functionality produces outputs that influence decisions about candidates or workers (shortlisting, scoring, suitability assessment), Article 22 UK GDPR applies if the decision is solely automated. The Data (Use and Access) Act 2025 (in force 5 February 2026) has expanded the lawful bases available but requires corresponding safeguards to be implemented and documented. Marchwood has not catalogued which HR/recruitment system features include AI functionality, and therefore cannot confirm which processing is solely automated and which involves meaningful human review.

CATEGORIES OF DATA AND OF DATA SUBJECT

Data subjects: candidates, placed contractors, and potentially client employees where Marchwood's systems interact with client HR data. Categories of data: name, contact details, employment history, qualifications, right-to-work status, health declarations, criminal record information, performance records. The same elevated-risk profile as the ATS applies where health or criminal record data is processed by AI components of HR systems placing into financial services and healthcare.

TRANSFER POSITION AND MECHANISM

Transfer position is unconfirmed for each HR/recruitment system vendor. Marchwood must identify every vendor in this category, confirm whether data is processed outside the UK, and verify that a UK-approved transfer mechanism (IDTA or adequacy decision) is in place for any offshore processing. This is an open gap.

RETENTION AND MODEL-TRAINING POSITION

No documented retention schedule is in place. Marchwood must establish and enforce retention periods for all data processed by HR and recruitment system AI features, consistent with UK GDPR Article 5(1)(e). Each vendor must provide written confirmation that candidate or worker data is not used to train or develop AI models beyond the scope of services provided to Marchwood. Absence of this confirmation is a compliance gap.

WHETHER A DPA IS IN PLACE AND WHAT IS MISSING

Marchwood has not confirmed that compliant Article 28 DPAs are in place with every HR/recruitment system vendor. Given that Marchwood has no record of which tools are approved, it is likely that some vendor relationships lack a DPA entirely. Marchwood must: (1) list every HR/recruitment platform with AI features in use; (2) obtain and review Article 28 DPAs for each; (3) confirm transfer mechanisms; (4) confirm model-training restrictions. Until complete, this category carries unquantified processor compliance risk.

OVERALL POSITION FOR THIS TOOL

High risk due to incomplete vendor inventory. Marchwood cannot currently confirm lawful processing, compliant Article 28 arrangements, or safe international transfers for this category of tool. A vendor audit is required before this category can be assessed as compliant.

AI-powered CRM or Sales Tools

GDPR COMPLIANCE POSITION — AI-POWERED CRM OR SALES TOOLS

Marchwood Talent | Prepared: 11 August 2026

CONTROLLER / PROCESSOR ROLES AND LAWFUL BASIS

Marchwood Talent is the data controller. CRM vendors with AI functionality (for example, AI-assisted lead scoring, automated outreach sequencing, predictive contact recommendations) act as data processors. The lawful basis for processing candidate and client contact data within the CRM is most likely Article 6(1)(f) (legitimate interests),

which requires a documented Legitimate Interests Assessment (LIA). Where AI features generate automated outputs that directly influence whether a candidate is contacted or presented to a client, the Article 22 question arises. If the AI scoring or ranking occurs without human review before a material decision, Article 22 applies. Marchwood has not documented this analysis.

CATEGORIES OF DATA AND OF DATA SUBJECT

Data subjects in the CRM context are primarily: (1) candidates — contact details, placement history, sector, skills, availability; and (2) client contacts — name, job title, employer, contact history. CRM data is less likely to include special category data than the ATS or HR systems, but Marchwood must confirm this, because candidate records migrated from or linked to the ATS may carry health or criminal record flags into the CRM. If special category data is present in the CRM, an Article 9 condition must be identified and documented.

TRANSFER POSITION AND MECHANISM

Many AI-powered CRM platforms (for example, Salesforce, HubSpot, Pipedrive with AI features) process data in the USA or have global infrastructure. Marchwood must confirm the data residency settings for its CRM vendor and verify the transfer mechanism. CRM vendors of scale typically offer IDTA-equivalent terms or operate under adequacy frameworks; however, Marchwood must obtain written confirmation of the specific mechanism applicable to its account and data region. This has not been confirmed.

RETENTION AND MODEL-TRAINING POSITION

Candidate and client contact data in the CRM must be subject to a documented retention schedule. For candidate data, the same principles apply as for ATS data (typically six to twelve months for inactive candidates, subject to any sector-specific requirement). For client contacts, retention should be tied to the duration of the commercial relationship plus any statutory minimum. Marchwood must confirm with its CRM vendor whether AI features use customer data for model training or product improvement, and obtain a written opt-out or contractual prohibition. CRM vendors' standard terms vary significantly on this point.

WHETHER A DPA IS IN PLACE AND WHAT IS MISSING

Marchwood must confirm whether a compliant Article 28 DPA is in place with its CRM vendor. Major CRM vendors typically include DPA terms in their commercial agreements or as a downloadable addendum; however, smaller or newer AI-native CRM tools may not. If Marchwood uses multiple CRM tools (authorised or shadow), each requires a separate DPA review. The absence of a documented approved-tool register means shadow CRM tools may be in use with no DPA at all. Marchwood must complete a CRM vendor audit as part of its broader shadow-AI remediation.

OVERALL POSITION FOR THIS TOOL

Moderate to high risk. The primary risk is the unconfirmed vendor landscape — Marchwood does not have a complete record of which CRM tools are in use. Where the CRM vendor is a major platform with standard DPA terms and IDTA mechanisms, the risk is manageable. Where shadow CRM tools are in use, the risk is unmitigated. A tool audit, DPA review, and legitimate interests assessment are required.

[ALL TOOLS — OVERALL COMPLIANCE POSITION]

OVERALL GDPR COMPLIANCE POSITION ACROSS ALL AI TOOLS

Marchwood Talent | Prepared: 11 August 2026

This section sets out the consolidated data protection position across all AI tools in scope and is intended for use in response to procurement due diligence requests, regulator enquiries, or insurer assessments.

SUMMARY POSITION

Marchwood Talent processes personal data — including special category data (health declarations, Article 9 UK GDPR) and criminal record data (Article 10 UK GDPR) — through multiple AI tools in the course of candidate recruitment and placement into financial services and healthcare. As at 11 August 2026, Marchwood does not have a documented AI tool register, does not have confirmed Article 28 Data Processing Agreements with all vendors, does not have a documented lawful basis for all AI-assisted processing, does not have a confirmed

transfer mechanism for all tools processing data outside the UK, and does not have internal policies governing which tools employees may use and for which purposes. This position exposes Marchwood to enforcement risk under UK GDPR, the Data (Use and Access) Act 2025, and the ICO's AI Auditing Framework. The maximum ICO fine is £17.5 million or 4% of global annual turnover, whichever is higher. The turnover-based limb cannot be calculated without Marchwood's financial figures; the statutory maximum is £17.5 million.

ARTICLE 22 AND AUTOMATED DECISION-MAKING

The ATS performs automated candidate ranking and shortlisting before any consultant review. This is solely automated decision-making producing a significant effect on candidates. UK GDPR Article 22(1) prohibits this unless a condition in Article 22(2) is met and the safeguards required under the Data (Use and Access) Act 2025 (in force 5 February 2026) are implemented. No Article 22 condition has been documented and no safeguards are in place. This is the single highest-priority compliance failure.

SPECIAL CATEGORY AND CRIMINAL RECORD DATA

Health declarations and criminal record information are processed through the ATS and potentially through ChatGPT (via CV pasting) and HR systems. Article 9 and Article 10 processing requires an explicit additional condition and, for Schedule 1 DPA 2018 conditions, an Appropriate Policy Document. Neither is in place. Processing special category data through a consumer ChatGPT account with no DPA is an active, unlawful disclosure.

SHADOW AI

Marchwood has no record of which tools are approved. Consultants are pasting CVs into ChatGPT without a controlled enterprise arrangement. The ICO's November 2024 audit outcomes on AI tools in recruitment identified ungoverned AI use as a key risk area. Shadow AI use — particularly involving special category data — is an enforcement priority.

COMPLAINTS PROCEDURE

The duty on controllers to operate a documented data protection complaints procedure and respond within set time limits came into force on 19 June 2026 under the Data (Use and Access) Act 2025. Marchwood must have a complaints procedure in place and must be able to demonstrate compliance with the prescribed response timescales. This must be documented and operationally active.

DATA SUBJECT RIGHTS

Candidates have rights under UK GDPR Articles 13–22, including the right to be informed about automated decision-making, the right of access, and (where Article 22 applies) the right to obtain human review, express their point of view, and contest the decision. Marchwood cannot currently fulfil these rights in relation to the ATS or confirm that privacy notices disclose AI-assisted processing. Privacy notices must be updated.

IMMEDIATE REMEDIATION PRIORITIES

1. Suspend the pasting of candidate data into consumer ChatGPT accounts immediately.
2. Document an Article 22 condition and implement the required safeguards for the ATS.
3. Identify and document an Article 9 condition and Appropriate Policy Document for all special category data processed by AI tools.
4. Produce an approved AI tool register and issue a shadow-AI prohibition policy.
5. Obtain and review Article 28 DPAs for every vendor.
6. Confirm international transfer mechanisms for every vendor processing data outside the UK.
7. Implement and document a data protection complaints procedure (required since 19 June 2026).
8. Update candidate privacy notices to disclose AI-assisted processing and automated decision-making.
9. Set and enforce retention schedules for all AI-processed personal data.
10. Obtain written confirmation from every vendor that candidate data is not used for AI model training.

Employee AI Policy Acknowledgement Form

Each member of staff signs one. Keep the signed copies — they are your evidence that the policy was communicated, which is the first thing asked for after an incident.

This form is completed by every Marchwood Talent employee before using any AI tool in the course of their work. Signed copies are retained as evidence that the Marchwood Talent AI Policy has been communicated to each individual. Retention of this evidence is a first-line requirement under the ICO AI Auditing Framework and supports Marchwood Talent's accountability obligations under UK GDPR Art. 5(2).

MARCHWOOD TALENT EMPLOYEE AI POLICY ACKNOWLEDGEMENT FORM

Version 1.0 | Effective: 11 August 2026

SECTION A — EMPLOYEE DETAILS

Full name: [FULL NAME]

Job title: [JOB TITLE]

Department / team: [DEPARTMENT]

Date of acknowledgement: [DATE]

SECTION B — CONFIRMATION OF POLICY READ

I confirm that I have read, understood, and will comply with the Marchwood Talent AI Acceptable Use Policy and all associated guidelines in full, including the sections covering candidate data, special-category data, automated decision-making, and shadow AI.

Initials: [INITIALS]

SECTION C — APPROVED AI TOOLS

I confirm that I am authorised to use only the tools listed below for Marchwood Talent work. Use of any AI tool not on this list (shadow AI) is prohibited and must be reported immediately under Section D.

Please tick each tool you are authorised to use in your role. Your line manager and the policy owner must confirm the applicable tools before this form is signed.

- ☐ Applicant Tracking System (ATS) — automated candidate ranking and shortlisting module
- ☐ ChatGPT / OpenAI — CV summarisation and content drafting only
- ☐ Microsoft 365 Copilot — internal documents and communications
- ☐ AI in HR or recruitment systems — as specified by your line manager
- ☐ AI-powered CRM or sales tools — business development use only

Additional approved tool (if any): [ADDITIONAL TOOL NAME OR "NONE"]

Scope limitation I acknowledge:

I understand that the ATS ranking and shortlisting function constitutes automated decision-making that may be subject to UK GDPR Art. 22 and the Data (Use and Access) Act, in force from 5 February 2026. I will not treat an ATS-generated ranking as a final hiring decision without human consultant review.

I understand that pasting candidate CVs, including health declarations or criminal record information, into ChatGPT or any other external generative AI tool may constitute a transfer of special-category personal data and is only permitted where the current approved data processing agreement and policy guidance

expressly authorise it.

Initials: [INITIALS]

SECTION D — INCIDENT REPORTING DUTY

I acknowledge that I have a duty to report the following to the Policy Owner and the Data Protection lead without delay and in any event within 24 hours of becoming aware:

1. Any use of an AI tool not listed in Section C (shadow AI).
2. Any AI output that may have introduced bias or discrimination into a recruitment or placement decision, including outputs that appear to disadvantage candidates on grounds protected under the Equality Act 2010 (age, disability, race, religion or belief, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership).
3. Any suspected or confirmed accidental disclosure of candidate personal data, including special-category data (health or criminal record information), to an AI tool or third-party system.
4. Any AI tool behaving in an unexpected or potentially harmful way.

Reporting contact: [POLICY OWNER NAME]

Reporting method: [EMAIL ADDRESS / INCIDENT LOG LOCATION]

I understand that failure to report a known incident promptly may increase Marchwood Talent's regulatory exposure, including under UK GDPR Art. 33 (72-hour breach notification to the ICO) and may result in disciplinary action.

Initials: [INITIALS]

SECTION E — EMPLOYEE DECLARATION AND SIGNATURE

I declare that:

- (a) I have read the Marchwood Talent AI Acceptable Use Policy in full;
- (b) I understand which AI tools I am authorised to use and the conditions attached to each;
- (c) I understand my reporting duties as set out in Section D;
- (d) I will not use AI tools to make or present as final any decision about a candidate or worker without human review, in compliance with UK GDPR Art. 22 and the Data (Use and Access) Act;
- (e) I understand that Marchwood Talent places candidates into financial services and healthcare, and that candidate data including health declarations and criminal record information is special-category or sensitive data under UK GDPR Art. 9 and Art. 10, requiring heightened care.

Employee signature: [EMPLOYEE SIGNATURE]

Date: [DATE]

SECTION F — POLICY OWNER COUNTERSIGNATURE

I confirm that the approved tools in Section C have been verified as correct for this employee's role, and that a copy of the current AI Acceptable Use Policy was provided to this employee prior to signature.

Policy owner name: [POLICY OWNER NAME]

Policy owner job title: [JOB TITLE]

Countersignature: [POLICY OWNER SIGNATURE]

Date: [DATE]

SECTION G — RETENTION NOTICE

The signed original of this form is filed in: [LOCATION — e.g. secure HR personnel file / named folder in SharePoint]

Retention period: This form is retained for the duration of the employee's employment plus 6 years from the date of leaving, in line with Marchwood Talent's data retention schedule and to support accountability obligations under UK GDPR Art. 5(2) and the ICO AI Auditing Framework.

Access is restricted to: HR, the Data Protection lead, the Policy Owner, and any regulator or auditor lawfully requesting it.

Full ICO AI Auditing Framework Assessment

The detailed assessment against the regulator's auditing framework — the document to produce if you are ever audited.

ICO AI Auditing Framework Assessment — Marchwood Talent

Prepared for: Marchwood Talent | Date: 11 August 2026 | Jurisdiction: United Kingdom

This assessment applies the ICO's AI Auditing Framework to Marchwood Talent's declared AI systems and use cases. It is structured to serve as the primary compliance record in the event of an ICO audit, regulatory enquiry, insurer due diligence, or client request. It covers all six assessment domains required under the framework and concludes with findings, remediation actions, and an overall maturity rating.

AI systems in scope: (1) Applicant tracking system (ATS) with automated candidate ranking and shortlisting; (2) ChatGPT / OpenAI, used by consultants to summarise CVs; (3) Microsoft 365 Copilot, used across HR, marketing, and data analysis functions; (4) AI-powered CRM and sales tools. All four systems process personal data. The ATS additionally produces outputs that directly affect individuals' access to employment opportunities, engaging the most stringent obligations under UK GDPR Article 22 and the Data (Use and Access) Act.

1. Governance and Accountability

Marchwood Talent currently has no documented AI governance policy, no register of approved tools, and no designated accountability owner for AI compliance. This is the most significant structural deficit identified in this assessment and it underlies nearly every other finding below.

Under UK GDPR Article 5(2) and Article 24, Marchwood Talent, as a data controller, must be able to demonstrate compliance with the data protection principles. The ICO's AI Auditing Framework makes clear that this obligation extends explicitly to AI systems that process personal data. Without a policy, an asset register, or a named accountability owner, Marchwood Talent cannot currently satisfy this accountability requirement.

The business places candidates into financial services and healthcare. Candidate data includes criminal record information (special category data under UK GDPR Article 9, or data processed under the regime applicable to criminal convictions under Article 10) and health declarations (Article 9 special category data). The processing of this data by AI systems, including the ATS and ChatGPT, requires an explicit lawful basis, a condition under Schedule 1 of the UK Data Protection Act 2018, and a documented Data Protection Impact Assessment (DPIA) under UK GDPR Article 35. No DPIA is in place.

Consultants are pasting CVs containing this sensitive data into ChatGPT without any assessed legal basis for that transfer, without contractual safeguards with OpenAI as a data processor, and without candidate awareness. This constitutes an uncontrolled data processing activity that exposes Marchwood Talent to direct regulatory liability.

Microsoft 365 Copilot and the AI-powered CRM tools have not been assessed or documented. It is unknown whether data processing agreements are in place, whether these tools access candidate or client personal data, and whether their outputs feed into decisions about people. This unknown exposure is a separate governance failure.

Immediate governance requirements: Marchwood Talent must appoint a named AI Compliance Owner (a senior individual with authority to enforce policy); produce an AI tool register listing every approved system, its data flows, its legal basis, and its risk classification; issue an interim prohibition on the use of any AI tool not on that register; and commission DPIAs for the ATS and for any AI tool processing special category data.

2. Lawfulness, Fairness, and the Bias Position

Lawfulness

The ATS performs automated ranking and shortlisting of candidates before any human consultant reviews them. Where that output determines or significantly influences which candidates are considered for a role, this is automated decision-making within the scope of UK GDPR Article 22. Article 22 prohibits solely automated decisions that produce legal or similarly significant effects on individuals unless one of three conditions is met: the decision is necessary for a contract, it is authorised by law with suitable safeguards, or the data subject has given explicit consent. Candidate shortlisting in a recruitment context produces a significant effect — exclusion from consideration for employment — and the Article 22 conditions must be identified and documented for each use case.

The Data (Use and Access) Act, with its Part 5 data protection provisions in force from 5 February 2026, has introduced wider lawful bases for solely automated decisions and associated safeguards. Marchwood Talent must assess whether the ATS's shortlisting function falls within these expanded provisions and, if so, document compliance with the accompanying safeguards, including the obligation to operate a complaints procedure. The complaints procedure duty came into force on 19 June 2026. Marchwood Talent has no complaints procedure in place and is therefore already in breach of this specific statutory duty.

The transfer of CV data into ChatGPT lacks any documented lawful basis. OpenAI is a US-headquartered entity. Any transfer of personal data to ChatGPT constitutes an international data transfer under UK GDPR Chapter V and must be covered by an approved transfer mechanism, such as the UK International Data Transfer Agreement or adequacy regulations. No such mechanism has been documented.

Fairness and Bias

The ICO's November 2024 audit outcomes on AI tools in recruitment identified bias in automated scoring and shortlisting as a primary concern. The ATS used by Marchwood Talent performs ranking and shortlisting automatically, but the business has no record of how the system's algorithm was built, what training data it used, whether that data was audited for demographic bias, or what protected characteristics under the Equality Act 2010 may be adversely affected by its outputs.

The Equality Act 2010 prohibits indirect discrimination: a provision, criterion, or practice that puts persons sharing a protected characteristic at a particular disadvantage compared with others and that cannot be justified as a proportionate means of achieving a legitimate aim. An ATS that systematically ranks candidates with gaps in employment history, non-UK educational qualifications, or names associated with particular ethnicities lower than others may produce indirect discriminatory outcomes. Marchwood Talent, as the entity deploying the system and making placements on the basis of its outputs, bears legal exposure for those outcomes regardless of whether the bias originates in the ATS vendor's model.

Marchwood Talent places into financial services and healthcare. The FCA's principles and the MHRA's guidance both require that AI-assisted processes in those sectors do not produce discriminatory outcomes in access to services. Discriminatory shortlisting of candidates for financial services or healthcare roles could therefore attract scrutiny from sector regulators in addition to the ICO and the Equality and Human Rights Commission.

No bias testing, demographic disparity analysis, or fairness monitoring has been conducted on the ATS. This must be rectified as a priority.

3. Transparency and Explainability of Each System

ATS (Automated Ranking and Shortlisting)

Candidates whose CVs are submitted through Marchwood Talent's recruitment process are subject to automated ranking before any human sees their application. UK GDPR Article 13 (where data is collected directly from the data subject) and Article 14 (where it is collected from third parties) require that individuals are informed, at the point of data collection, that their data will be subject to automated decision-making, the logic involved, and the significance and envisaged consequences for them. Article 22(3) additionally requires that, where automated decision-making applies, the data subject must be given meaningful information about the logic involved and the right to obtain human review.

Marchwood Talent's privacy notice has not been reviewed as part of this assessment, but the business has confirmed no policy is in place. It is highly unlikely that the current candidate-facing documentation satisfies Articles 13, 14, or 22(3) transparency requirements. Candidates are almost certainly unaware that their application is ranked by an algorithm before a human consultant engages with it.

Explainability is also an internal requirement. Consultants must be able to understand why the ATS has ranked a candidate highly or excluded them, in order to exercise meaningful human oversight. If the ATS is a black-box system whose scores cannot be explained, Marchwood Talent cannot credibly argue that human review of those scores constitutes genuine oversight rather than rubber-stamping.

ChatGPT / OpenAI

Candidates are not informed that their CV data, including sensitive declarations, is being processed by ChatGPT. There is no transparency notice, no candidate consent, and no record of what data has been shared or what outputs were generated. The ICO's guidance on generative AI is clear that individuals whose data is processed by these tools retain full UK GDPR rights and must be informed of that processing. This is a transparency failure affecting every candidate whose CV has been pasted into ChatGPT.

Microsoft 365 Copilot

Copilot is used for marketing content, HR functions, and data analysis. Where Copilot processes personal data — for example, if HR-related prompts contain employee or candidate information, or if data analysis queries include identifiable records — the same transparency obligations apply. There is no evidence that Marchwood Talent has assessed what personal data Copilot accesses or that staff have been instructed not to input personal data without an assessed lawful basis.

AI-Powered CRM and Sales Tools

These tools are in scope but have not been assessed or documented by Marchwood Talent. Without knowing what data they process and what decisions they inform, a full transparency assessment cannot be completed. This gap must be closed. Until it is, these tools should be treated as unassessed and potentially non-compliant.

4. Security and the AI-Specific Attack Surface

Marchwood Talent processes criminal record information and health declarations via AI systems. This is among the most sensitive personal data that a UK recruitment business can hold, and the AI-specific security risks associated with its processing are materially elevated compared with standard personal data.

The primary security concern identified is the uncontrolled transfer of special category data into ChatGPT. OpenAI's consumer and API products process user inputs on infrastructure outside Marchwood Talent's control. Unless Marchwood Talent has an enterprise agreement with OpenAI that includes a Data Processing Agreement, a UK-compatible transfer mechanism, and contractual restrictions on data use for model training, the business has no assurance that candidate data submitted to ChatGPT is not retained, used to train future models, or accessible to OpenAI staff. The ICO has confirmed that personal data submitted to third-party AI tools is subject to UK GDPR obligations on the controller who submits it. Marchwood Talent is that controller.

AI-specific attack vectors that Marchwood Talent must address include: prompt injection (where malicious content in a CV or data input manipulates the AI's output, potentially causing a consultant to act on false information); data extraction via model memorisation (where sensitive data input into a generative AI system may be reproduced in outputs to other users); and model inversion or inference attacks against the ATS if it exposes an API. These are not theoretical risks — the ICO confirmed in August 2026 that it is monitoring reports of AI models compromising real-world systems during security evaluations.

The absence of an approved tool register means that shadow AI use — employees using personal accounts for ChatGPT, or using other unapproved tools — cannot be detected or controlled. This is the shadow AI risk Marchwood Talent has itself identified as a concern, and it is confirmed by the lack of any policy or monitoring framework.

Markerwood Talent must implement the following security controls: a Data Processing Agreement with OpenAI (or a prohibition on ChatGPT use until one is in place); a UK-compatible international transfer mechanism for any AI tool hosted outside the UK; a staff policy prohibiting the input of personal data, especially special category data, into unapproved AI tools; technical controls (such as data loss prevention rules) to enforce that prohibition where technically feasible; a security review of the ATS including assessment of its data retention, access controls, and API exposure; and inclusion of AI-specific scenarios in Marchwood Talent's existing (or to-be-created) incident response plan.

5. Individual Rights, Including Automated Decision-Making

UK GDPR provides data subjects with a set of rights that Marchwood Talent must be able to fulfil in respect of all AI-processed personal data. These rights are not suspended because personal data is processed by an AI system — they apply with equal or greater force.

Right to be informed (Articles 13 and 14): As noted under transparency, candidates are not currently informed that automated ranking is applied to their data or that their CV may be processed by third-party AI tools. This right is being systematically breached.

Right of access (Article 15): A candidate submitting a Subject Access Request is entitled to receive a copy of all personal data held about them, including ATS scores, ranking outputs, and any ChatGPT summaries if those were retained. Marchwood Talent has no system for identifying, collating, or disclosing AI-generated outputs in response to a SAR. This is a compliance gap.

Right to object (Article 21): Where processing is based on legitimate interests, data subjects have the right to object. Marchwood Talent must be able to handle and respond to objections to AI-assisted processing.

Rights in relation to automated decision-making (Article 22 and Data (Use and Access) Act): Where the ATS's shortlisting constitutes a solely automated decision with significant effect, candidates have the right to: obtain human review of the decision; express their point of view; and obtain an explanation of the decision. The Data (Use and Access) Act's expanded framework for automated decisions, in force from 5 February 2026, provides wider lawful bases for such processing but imposes mandatory safeguards, including the obligation — in force from 19 June 2026 — for controllers to operate a complaints procedure for data protection matters and to respond within set time limits. Marchwood Talent has no complaints procedure. This is a specific, current breach of a statutory duty that has been in force for nearly two months as at the date of this assessment.

Right to erasure (Article 17): Candidates may request deletion of their data. If ATS outputs or ChatGPT summaries are held outside the main candidate record (for example, in a consultant's email or in ChatGPT's history), Marchwood Talent may be unable to locate and delete all relevant data. This is both a rights compliance risk and an ongoing security risk.

Special category data rights: The processing of health and criminal record data by AI requires a specific Schedule 1 condition under the Data Protection Act 2018 in addition to an Article 9 condition. The most likely applicable condition for recruitment purposes is substantial public interest or the exercise of rights in the field of employment. Relying on this condition requires an Appropriate Policy Document to be in place. No such document exists at Marchwood Talent.

6. Findings, Remediation Actions, and Owners

Finding 1 — No AI governance policy or approved tool register

Severity: Critical. Marchwood Talent cannot demonstrate compliance with UK GDPR Article 24 or the ICO's accountability principle. Every AI tool in use is operating without documented legal basis, risk assessment, or oversight.

Remediation: Appoint a named AI Compliance Owner within 14 days. Produce an AI tool register covering all four in-scope systems within 30 days. Issue an interim staff notice prohibiting use of any tool not on the register.

Owner: Managing Director / designated AI Compliance Owner.

Finding 2 — No DPIA for the ATS or any AI tool processing special category data

Severity: Critical. UK GDPR Article 35 mandates a DPIA for processing likely to result in high risk, which automated decision-making on special category data unambiguously is. Absence of a DPIA is itself a breach and prevents identification of further risks.

Remediation: Commission and complete a DPIA for the ATS within 45 days. Commission a DPIA for ChatGPT use within 30 days. Both must be completed before those tools continue to process special category data.

Owner: AI Compliance Owner with external DPIA support.

Finding 3 — No complaints procedure under the Data (Use and Access) Act

Severity: High. The duty to operate a complaints procedure and respond to data protection complaints within set time limits came into force on 19 June 2026. Marchwood Talent is in breach of this statutory duty now.

Remediation: Implement a documented complaints procedure within 14 days, covering AI-related data protection complaints, and train all staff on its operation.

Owner: AI Compliance Owner.

Finding 4 — ChatGPT used to process special category candidate data without lawful basis, DPA, or transfer mechanism

Severity: Critical. The transfer of criminal record and health data into ChatGPT without a Data Processing Agreement, an international transfer mechanism, or candidate transparency is a multi-limb breach of UK GDPR Articles 5, 9, 13/14, 28, and Chapter V.

Remediation: Suspend the use of ChatGPT for CV processing immediately pending completion of a DPIA and execution of a UK-compliant Data Processing Agreement and international transfer mechanism with OpenAI. If an enterprise agreement cannot be secured, the use case must be discontinued.

Owner: AI Compliance Owner; IT lead for contract execution.

Finding 5 — ATS automated shortlisting: Article 22 conditions not documented

Severity: Critical. Automated shortlisting that determines which candidates a consultant considers produces a significant effect. The legal basis under Article 22 and the Data (Use and Access) Act has not been identified or documented, and candidates have not been informed.

Remediation: Legal basis analysis to be completed within 30 days. Candidate privacy notice to be updated to include automated decision-making disclosures. Human review protocol to be documented and implemented.

Owner: AI Compliance Owner; legal adviser.

Finding 6 — No bias or fairness testing on the ATS

Severity: High. Failure to test for discriminatory outputs exposes Marchwood Talent to Equality Act 2010 liability and ICO regulatory action, and creates risk for the financial services and healthcare clients into which candidates are placed.

Remediation: Request vendor documentation of training data, bias audits, and fairness metrics within 30 days. Commission independent demographic disparity analysis of historical shortlisting outputs within 60 days. Establish ongoing monitoring.

Owner: AI Compliance Owner; ATS vendor.

Finding 7 — No transparency to candidates about AI processing

Severity: High. Candidates are not informed of automated ranking or third-party AI CV processing, in breach of UK GDPR Articles 13, 14, and 22(3).

Remediation: Update the candidate privacy notice and application process disclosures within 30 days. Include the logic of automated processing, its significance, and the right to human review.

Owner: Marketing / operations lead; AI Compliance Owner.

Finding 8 — Shadow AI: no controls on unapproved tool use

Severity: High. Without a policy or technical controls, employees may be using personal ChatGPT accounts, consumer AI tools, or other unapproved systems with candidate data. This is undetectable and uncontrollable in the current environment.

Remediation: Publish an AI Acceptable Use Policy within 30 days specifying approved tools and prohibiting unapproved tool use for personal data. Implement technical controls (DNS filtering, DLP rules) within 60 days. Include AI in staff induction and annual training.

Owner: IT lead; AI Compliance Owner.

Finding 9 — Microsoft 365 Copilot and CRM tools: unassessed

Severity: Medium. These tools are in scope and may process personal data, but have not been assessed. Their risk profile is unknown.

Remediation: Complete a data flow mapping exercise for Copilot and the CRM tool within 45 days. Assess whether personal data is processed and, if so, document the lawful basis, DPA, and transparency obligations.

Owner: IT lead; AI Compliance Owner.

Finding 10 — No Appropriate Policy Document for special category data

Severity: High. Processing criminal record and health data for recruitment purposes requires an Appropriate Policy Document under the Data Protection Act 2018 Schedule 1. None exists.

Remediation: Draft and adopt an Appropriate Policy Document within 30 days covering all Schedule 1 conditions relied upon.

Owner: AI Compliance Owner; legal adviser.

7. Overall Maturity Rating and Basis

Overall Maturity Rating: Initial / Ad Hoc (Level 1 of 5)

This rating reflects the ICO AI Auditing Framework's five-level maturity model. Level 1 — Initial — is assigned where AI governance is absent or entirely unstructured, compliance activities are reactive rather than planned, accountability is unassigned, and the organisation cannot demonstrate compliance in any material area of the framework.

Marchwood Talent meets Level 1 criteria across all six assessment domains. There is no policy, no register, no DPIA, no bias testing, no candidate transparency, no complaints procedure, no staff training, and no security controls specific to AI. Several of these gaps constitute current, active breaches of UK law, not merely future risks.

The maximum financial exposure under UK GDPR is £17.5 million or 4% of global annual turnover, whichever is higher. For a business of Marchwood Talent's size, the turnover-based limb cannot be computed without actual turnover figures, but the statutory maximum of £17.5 million applies as the ceiling for the most serious infringements. The processing of special category data by AI systems without lawful basis, without DPIAs, and without candidate transparency represents the category of infringement to which the ICO's highest penalty tier applies. The November 2024 ICO audit of AI in recruitment demonstrates that this is an active enforcement priority, not a theoretical one.

To reach Level 2 — Developing — Marchwood Talent must complete the critical findings (1, 2, 3, 4, 5) within the timeframes specified, demonstrating that governance structures, lawful bases, and immediate safeguards are in place. To reach Level 3 — Defined — the business must complete all ten findings, implement ongoing monitoring, and embed AI risk into its annual data protection review cycle.

A reassessment against this framework should be scheduled for no later than 90 days from the date of this document, by which point all critical and high findings should be closed or have documented remediation plans with evidence of progress.

Employment AI Procedures

Using AI in recruitment, monitoring or management decisions — the highest-risk use in most businesses, and the most regulated.

1. Purpose and Scope

This document sets out Marchwood Talent's binding procedures for every use of artificial intelligence in recruitment, candidate assessment, and employment-related decisions. It applies to all employees, consultants, and third-party suppliers who use AI tools on behalf of Marchwood Talent. It forms part of Marchwood Talent's wider AI Compliance Pack and must be read alongside the Data Protection Policy and the Approved AI Tools Register.

The procedures are grounded in UK GDPR Article 22 (automated decision-making and profiling), the Data (Use and Access) Act 2025 (Part 5 provisions in force from 5 February 2026, including the wider lawful bases for solely automated decisions and the safeguards that accompany them, and the complaints-procedure duty in force from 19 June 2026), the ICO AI Auditing Framework, and the Equality Act 2010. Marchwood Talent places candidates into financial services and healthcare, sectors in which candidates routinely provide criminal record disclosures and health declarations. Those categories of data attract the highest level of protection under UK GDPR Article 9 (special category data) and Article 10 (criminal convictions data), and that elevation in risk runs through every section of this document.

Non-compliance with these procedures may expose Marchwood Talent to ICO fines of up to £17.5 million or 4% of global annual turnover (whichever is higher), Equality Act enforcement by the Employment Tribunal or County Court, and reputational damage with the regulated-sector clients it serves. Compliance with this document is therefore mandatory, not optional.

2. AI Tools Currently in Use for Employment and Recruitment Purposes

Marchwood Talent currently operates the following AI tools in contexts that affect candidates or workers. Each is described with its function and the point in the recruitment workflow at which it operates.

Applicant Tracking System (ATS) with automated ranking and shortlisting. The ATS ingests applications and automatically scores, ranks, and shortlists candidates before any consultant reviews them. This is the highest-risk tool in the business because it makes or heavily influences decisions about which candidates progress. Where the ATS produces a shortlist without meaningful consultant input before that list is acted upon, it constitutes solely automated decision-making within the scope of UK GDPR Article 22 and the Data (Use and Access) Act 2025 Part 5.

ChatGPT / OpenAI. Consultants currently paste candidate CVs into ChatGPT to generate summaries. This practice transfers personal data — including, in the context of financial services and healthcare placements, potentially sensitive information — to OpenAI's systems. This is not a sanctioned data-sharing arrangement and represents a live GDPR breach risk as well as a shadow-AI risk. The position on this tool is addressed specifically in Section 7.

Microsoft 365 Copilot. Copilot is in use across the business and may be applied to recruitment-related documents, emails, and spreadsheets. Its use in processing candidate or employee data is subject to these procedures.

AI in HR or recruitment systems. Beyond the ATS, any AI-assisted functionality embedded in HR platforms used to manage employee performance or conduct is in scope. Where no such functionality is currently active, this section records that position explicitly so that any future activation triggers a review under these procedures before deployment.

AI-powered CRM or sales tools. Where CRM tools surface or score candidate profiles for business development or re-engagement purposes, they process personal data and are in scope. Consultants must not use CRM AI-scoring outputs as a substitute for individual assessment.

3. Discrimination Risk and Indirect Discrimination

The Equality Act 2010 prohibits direct and indirect discrimination on the basis of protected characteristics including age, disability, race, sex, pregnancy and maternity, religion or belief, sexual orientation, gender reassignment, and marriage and civil partnership. AI tools can produce indirect discrimination — where a provision, criterion, or practice that appears neutral on its face puts a group sharing a protected characteristic at a particular disadvantage — without any discriminatory intent. The ATS ranking algorithm is the most significant source of this risk at Marchwood Talent.

Ranking models trained on historical hiring data can encode past human biases. If, for example, the ATS was trained on data from a sector that historically under-represented women or ethnic minorities in senior roles, the model may systematically score those groups lower. Because Marchwood Talent places into financial services and healthcare — sectors with documented demographic imbalances — this risk is elevated.

Marchwood Talent requires the following testing and monitoring regime. Before the ATS ranking feature is used for any new client vacancy, the Compliance Lead must request from the ATS supplier the most recent bias audit report, including information on training data composition, protected-characteristic testing outcomes, and any disparate-impact findings. This report must be reviewed and retained. Where no such report is available from the supplier, the ATS ranking feature must not be used for that vacancy until one is obtained or the tool is replaced.

Quarterly, the Compliance Lead will extract shortlisting data from the ATS and conduct a disparate-impact analysis, comparing the pass-through rates of candidates by gender and, where data is available and lawfully processed, by age band and ethnicity. If any group's pass-through rate is materially lower than the overall rate without a legitimate, proportionate justification, the algorithm must be suspended for that vacancy type pending investigation. Results of each quarterly review must be recorded and retained for four years.

Consultants must not use ChatGPT or any unapproved tool to re-rank, re-score, or filter candidates in a way that replicates automated shortlisting. Any manual review process must apply the same criteria consistently across all candidates.

4. Reasonable Adjustments and Accessibility of AI-Assisted Processes

The Equality Act 2010 requires Marchwood Talent to make reasonable adjustments where a provision, criterion, or practice — including any AI-assisted process — places a disabled person at a substantial disadvantage compared with persons who are not disabled. Because candidates cannot always identify in advance that an AI process is involved, the duty to consider adjustments must be proactive, not reactive.

For any vacancy where the ATS applies automated scoring or ranking, the candidate-facing application process must include a clear invitation to notify Marchwood Talent of any requirement for adjustment, with a named contact and a specific email address. This invitation must appear at the point of application, not only in a general privacy notice.

Where a candidate discloses a disability or adjustment need, a consultant must manually review that candidate's application independently of the ATS-generated score. The manual review applies the same substantive criteria but is conducted by a human without reference to the AI ranking. The outcome of the manual review governs whether the candidate progresses, not the ATS score. This review must be documented.

AI-generated CV summaries produced via Copilot or any approved tool must not be the sole basis on which a consultant forms a view of a candidate with a disclosed disability. Where a summary omits or mischaracterises information relating to adjusted working patterns, employment gaps attributable to ill-health, or non-standard career paths, the consultant must return to the original CV.

Health declarations received in connection with financial services or healthcare placements are special category data under UK GDPR Article 9. They must not be entered into ChatGPT or any AI tool outside Marchwood Talent's approved, contracted data-processing environment. Processing of such declarations must have an explicit legal basis under Article 9(2), which in the employment and recruitment context is most likely Article 9(2)(b) (employment law obligations) supported by a Schedule 1 condition under the Data Protection Act 2018.

5. What Candidates and Staff Are Told, and When

Transparency is a requirement of UK GDPR Articles 13 and 14, and the right to be informed about solely automated decision-making is specifically reinforced by Article 22(3) and the corresponding provisions of the Data (Use and Access) Act 2025. Marchwood Talent currently has no documented disclosure practice. This section establishes the mandatory minimum.

At the point of application for any vacancy where the ATS applies automated ranking or shortlisting, candidates must be told: that an automated system will assess and rank their application before a human consultant reviews it; the logic involved (in plain English, for example that the system scores against skills, experience, and role-specific criteria specified by the client); the significance of that processing for their application (it determines whether they reach the human-review stage); and their right to request human review, to contest the outcome, and to obtain a meaningful explanation of the decision. This disclosure must appear in the candidate-facing application or in a privacy notice linked prominently from it, not buried in a general website footer.

Where a candidate is rejected at the automated stage without any human review, Marchwood Talent must inform them of that fact within a reasonable period, provide the categories of criteria the system applied, and inform them of their right to request human reconsideration. Rejection communications must not imply that a human assessed and decided. That would be a misleading statement inconsistent with UK GDPR Article 5(1)(a) (lawfulness, fairness, and transparency).

For employees of Marchwood Talent itself, where Microsoft 365 Copilot or any AI tool is used in performance management or monitoring, staff must be informed via a written notice before that use commences. The notice must describe what data is processed, for what purpose, how decisions or recommendations informed by AI are made, and who makes the final decision. This notice must be issued before the tool is activated for that purpose, not retrospectively.

Marchwood Talent must maintain a log of all candidate and employee transparency notices issued, including the date, the version of the notice, and the vacancy or process to which it related.

6. Human Review of Decisions Affecting a Person

UK GDPR Article 22(1) provides that a data subject has the right not to be subject to a decision based solely on automated processing which produces a significant effect concerning them. The Data (Use and Access) Act 2025 Part 5 provisions, in force from 5 February 2026, introduce wider lawful bases for solely automated decisions but do not remove the obligation to have safeguards in place, including the right to obtain human review. These provisions are directly applicable to Marchwood Talent's ATS.

Marchwood Talent's position is that no candidate may be finally rejected, progressed to a client, or placed on a client shortlist on the basis of an ATS score alone. Every ATS-generated shortlist must be reviewed by a named consultant before it is acted upon. The consultant must apply independent professional judgement, must be capable of overriding the ATS ranking, and must document the basis for any departure from the ATS output.

Where a candidate requests human review of an automated decision — which they are entitled to do under Article 22(3) and the Data (Use and Access) Act 2025 — that request must be acknowledged within five working days and substantively completed within one calendar month. The review must be conducted by a consultant who was not involved in the original automated process. The outcome, reasoning, and any change to the original decision must be recorded.

Marchwood Talent must designate at least one senior employee as the Human Review Officer for each operational team. Their identity must be disclosed to candidates on request. They are responsible for ensuring reviews are completed on time and to the required standard.

For employee-facing uses of AI within Marchwood Talent itself (for example, if Copilot is used to assist in drafting performance reviews or attendance analysis), no output of that AI process may be used as a final determination without a line-manager review and sign-off. The line manager must confirm in writing that they have considered the AI output critically, not adopted it uncritically.

7. Shadow AI and the Use of ChatGPT for CV Summarisation

Marchwood Talent has confirmed that consultants currently paste candidate CVs into ChatGPT to generate summaries. This practice is not covered by any data processing agreement between Marchwood Talent and OpenAI, is not listed in Marchwood Talent's approved tools register (which did not exist at the time of this compliance review), and results in personal data — including, for healthcare and financial services candidates, information that may constitute special category data or criminal convictions data — being transferred to a third-party system outside Marchwood Talent's control. This is a breach of UK GDPR Article 28 (processor requirements), Article 9, and Article 46 (where data may be processed outside the UK). It must stop immediately.

With effect from the date this document is approved by senior management, no consultant may paste candidate personal data into ChatGPT or any other AI tool that is not on the Approved AI Tools Register. The Register must be established as a parallel action and must, at minimum, specify: the tool name; the supplier; whether a data processing agreement is in place; whether the tool is approved for special category data; and which use cases are permitted.

If Marchwood Talent wishes to use an AI summarisation tool for CVs, it must first: identify a tool offered under terms that include a compliant UK GDPR Article 28 data processing agreement; assess whether that tool transfers data outside the UK and, if so, ensure appropriate safeguards under Article 46; and conduct a Data Protection Impact Assessment before deployment, given the special category data involved.

Until a compliant tool is approved and the DPIA completed, CV summarisation must be performed manually by the consultant. This is not a transitional suggestion — it is a mandatory interim requirement.

Shadow AI — employees using any AI tool not on the Approved Register — must be addressed through mandatory training for all staff, a clear written instruction from senior management, and a process for consultants to propose new tools for review rather than adopting them unilaterally. Any consultant found using an unapproved tool after the date of this document's approval will be subject to disciplinary proceedings.

8. Records Kept and Retention Periods

Marchwood Talent must maintain records sufficient to demonstrate compliance with UK GDPR, the Data (Use and Access) Act 2025, the Equality Act 2010, and the ICO AI Auditing Framework. Records must be capable of responding to an ICO investigation, a Subject Access Request, an Equality Act claim, or a dispute raised through Marchwood Talent's complaints procedure (the duty to operate which came into force on 19 June 2026 under the Data (Use and Access) Act 2025).

The following records must be created and retained. ATS shortlisting records: for each vacancy, a copy of the criteria entered into the ATS, the ranked output, the consultant's review notes, and the final shortlist as provided to the client. Retained for four years from the date the vacancy was closed. This period reflects the Equality Act limitation period for civil claims (six months from the act complained of to Employment Tribunal, but up to six years in County Court for some discrimination claims) and the ICO's expectation of accountability records.

Bias audit reports from the ATS supplier: retained for the life of the contract with that supplier plus two years. Quarterly disparate-impact analysis results: retained for four years. DPIA records for any AI tool processing special category data: retained for the life of the tool's use plus three years. Candidate transparency notices and the dates

on which they were issued: retained for four years. Human review requests, outcomes, and correspondence: retained for four years from the date of the review.

Records of the Approved AI Tools Register, including when tools were added, removed, or had their permitted scope changed: retained indefinitely as a governance record. Training records confirming that all employees received mandatory AI and data protection training: retained for the duration of employment plus three years.

All records must be stored in Marchwood Talent's controlled systems. They must not be stored solely in personal email accounts or personal devices. Access must be restricted to those with a legitimate need. The Compliance Lead is responsible for ensuring the retention schedule is applied and that records are not deleted before their minimum retention period expires.

9. Complaints Procedure for AI-Related Decisions

The Data (Use and Access) Act 2025 imposes a duty on controllers to operate a complaints procedure and respond to data protection complaints within set time limits. This duty came into force on 19 June 2026. Marchwood Talent must comply with it as of that date.

Any candidate or employee who believes that an AI-assisted process has produced an inaccurate, unfair, or discriminatory outcome may submit a complaint to Marchwood Talent's designated Compliance Lead. Complaints must be submitted in writing (including by email) and must describe the decision complained of, the ground of complaint, and any evidence the complainant wishes to rely upon.

Marchwood Talent will acknowledge the complaint within five working days. A substantive written response will be provided within one calendar month of receipt, with the option to extend by a further two months where the complaint is complex, provided the complainant is notified of the extension and its reason within the first month.

The substantive response will explain: whether AI processing was involved in the decision; what the AI system did; what human review took place; whether the outcome will be reconsidered; and the complainant's right to escalate to the ICO at ico.org.uk if they remain dissatisfied. Complainants who believe they have been discriminated against on grounds of a protected characteristic may also refer their complaint to the Equality and Human Rights Commission or bring a claim in the Employment Tribunal or County Court under the Equality Act 2010.

All complaints and responses must be logged and retained in accordance with Section 8 of this document.

10. Document Control and Review

This document was prepared on 11 August 2026 and approved by Marchwood Talent senior management on the date shown in the document control log. It must be reviewed in full no later than 11 August 2027, or sooner if: a new AI tool is adopted; the ATS supplier changes its ranking algorithm; a new regulatory instrument or ICO guidance materially affecting recruitment AI comes into force; or a complaint, audit finding, or enforcement action identifies a gap.

Ownership of this document rests with the Compliance Lead. Day-to-day compliance responsibilities rest with all employees who use AI tools in the course of their work. Senior management is accountable for ensuring adequate resource is allocated to implement and maintain these procedures.

This document supersedes any previous informal practice regarding AI use in recruitment. In the absence of any previous policy, it constitutes the foundational record of Marchwood Talent's intent and obligations in this area.

Automated Decision-Making Notices and Opt-Out Procedures

The notices you give when a decision is made by a machine, and the route out that the law requires you to offer.

1. Scope and Legal Framework

This document applies to Marchwood Talent and governs every situation in which an automated system makes or materially influences a decision about an individual. It takes effect from 11 August 2026 and must be reviewed whenever a tool, workflow or placement sector changes.

The primary legal basis is UK GDPR Article 22, which gives data subjects the right not to be subject to a decision based solely on automated processing that produces a legal or similarly significant effect. The Data (Use and Access) Act 2025 (Part 5 provisions in force from 5 February 2026) reforms the lawful bases available for solely automated decisions and introduces mandatory safeguards that Marchwood Talent must now operate. Those safeguards include the right to obtain human intervention, to express a point of view and to contest the decision. The duty on controllers to operate a complaints procedure and to respond to data protection complaints within set time limits came into force on 19 June 2026 and applies to all human-review requests made under this document.

Because Marchwood Talent places candidates into financial services and healthcare, candidate records frequently contain special-category data (health declarations) and criminal record data. Both categories attract heightened obligations under UK GDPR Articles 9 and 10 in addition to the Article 22 regime. The Equality Act 2010 runs alongside: any automated ranking or shortlisting that produces a disparate impact on a protected characteristic constitutes potential indirect discrimination, and that risk is not cured merely by offering a human review unless the review itself is substantive and documented.

The ICO's maximum fine is £17,500,000 or 4% of global annual turnover, whichever is higher. The turnover-based limb cannot be computed without Marchwood Talent's figures, but the fixed ceiling of £17,500,000 illustrates the materiality of non-compliance for a business of 11–50 employees.

2. Automated and Significantly Automated Decisions at Marchwood Talent

Two distinct processing activities at Marchwood Talent fall within the scope of Article 22 and the Data (Use and Access) Act 2025 reforms.

First, the applicant tracking system (ATS) ranks and shortlists candidates automatically before any consultant reviews the profile. Where the ATS determines that a candidate does not appear in the shortlist presented to a consultant, that candidate is effectively excluded from further consideration without any human having assessed their application. This is a decision based solely on automated processing that produces a similarly significant effect on the candidate's ability to obtain employment. It engages Article 22 in full.

Second, consultants routinely paste candidate CVs into ChatGPT to generate summaries. Where a consultant uses that summary as the primary or sole basis for deciding whether to progress, reject or present a candidate — without independently reading the underlying CV — the processing is significantly automated even though a human receives the output. The human step is nominal rather than substantive, which means Article 22 safeguards still apply. Where the consultant does read the full CV and uses the ChatGPT summary only as an aide-memoire, the decision is not solely automated; however, this distinction must be evidenced at the time, not reconstructed later.

Microsoft 365 Copilot, the AI-powered CRM and any AI features embedded in HR or recruitment systems may assist in drafting communications or analysing pipeline data. To the extent that those outputs are used to score, rank or recommend individual candidates without substantive human review, they are treated as significantly automated decisions and fall within this document. Marchwood Talent must audit each tool's actual decision-influencing role and update this document accordingly.

3. Notice Wording — ATS Automated Shortlisting

The following notice must be provided to every candidate at the point of application, before the ATS processes their data.

NOTICE OF AUTOMATED DECISION-MAKING — CANDIDATE SHORTLISTING

Marchwood Talent uses an automated applicant tracking system to rank and shortlist candidates before a consultant reviews applications. This means that an automated system may determine whether your application is included in the shortlist presented to one of our consultants. This constitutes automated decision-making that may have a significant effect on your ability to progress in this process.

You have the right to: (a) request that a named Marchwood Talent consultant reviews your application personally, without relying on the automated ranking; (b) express your point of view about your application directly to that consultant; and (c) contest the outcome if you believe the automated ranking is inaccurate or unfair.

To exercise any of these rights, please contact us using the details in Section 5 of this document. We will acknowledge your request within five working days and complete the human review within 15 calendar days.

Where your application involves health information or criminal record data, those details will not be used as ranking criteria by the automated system unless we have a specific lawful basis to do so and have informed you separately.

This notice must be incorporated into Marchwood Talent's candidate-facing application form and privacy notice. It may not be buried in general terms and conditions.

4. Notice Wording — ChatGPT CV Summarisation

The following notice must be provided to every candidate whose CV is summarised using ChatGPT or any other large language model, at the latest at the point their data is first shared with such a tool. Where the consultant decides after reading the CV that they will use ChatGPT to assist their review, the notice must be sent before any decision is communicated to the candidate.

NOTICE OF AI-ASSISTED PROCESSING — CV REVIEW

Marchwood Talent may use an AI language tool (currently ChatGPT, operated by OpenAI) to produce a summary of your CV to assist one of our consultants in reviewing your application. Where the consultant's decision to progress, hold or decline your application is based primarily on that AI-generated summary rather than a full independent reading of your CV, this processing is treated as significantly automated and you have the same rights as those described in the ATS Shortlisting Notice above.

You have the right to request that a consultant reviews your original CV without reference to any AI-generated summary, to express your point of view, and to contest any outcome you consider unfair or inaccurate.

Please note: your CV and any personal data it contains will be processed by OpenAI's systems when this tool is used. Marchwood Talent operates a data processing agreement with OpenAI for this purpose. If you object to your data being processed in this way, please contact us before your CV is submitted and we will accommodate your request.

This notice must be delivered by email to the candidate's confirmed address before the CV is pasted into ChatGPT. A sent-email record constitutes proof of delivery for the purposes of Section 7 below.

5. How to Make an Opt-Out or Human-Review Request

Marchwood Talent designates a single point of contact for all automated decision-making requests. As at 11 August 2026, this is the most senior consultant or, where a data protection lead has been appointed, that individual. All requests must be directed to: compliance@marchwoodtalent.co.uk (to be activated by Marchwood Talent on adoption of this document). A telephone number must also be published in the candidate-facing notice; email alone is insufficient where a candidate may lack ready access to email.

A candidate may make a request at any point in the process: before the ATS runs, after receiving a rejection, or after receiving an AI-assisted summary decision. There is no requirement for the candidate to use formal language. Any communication that expresses dissatisfaction with an automated outcome, asks for a person to look at their application, or questions how a decision was reached, must be treated as a human-review request and routed immediately to the designated contact.

Consultants who receive a request directly — whether by telephone, email or through the CRM — must forward it to the designated contact within one working day. They must not attempt to resolve it themselves by re-running the ATS or producing a second ChatGPT summary. The response must involve a substantive, documented human review as described in Section 6.

Where a candidate is located in a jurisdiction whose local law creates additional rights (for example, EU residents whose data is processed in connection with roles that have an EU nexus), Marchwood Talent must consider those rights separately. This document governs UK-resident candidates and UK-processed data.

6. Response Deadlines and Responsible Individuals

All human-review requests must be acknowledged in writing within five working days of receipt. The acknowledgement must name the consultant who will conduct the review and give the date by which the review will be completed.

The substantive human review must be completed and communicated to the candidate within 15 calendar days of the date the request was received. This timeline reflects the obligation under the Data (Use and Access) Act 2025 complaints-procedure duty (in force 19 June 2026) and the reasonable expectations set by the ICO's AI auditing framework for recruitment. In complex cases involving special-category data (health declarations) or criminal record data, the 15-day period must still be met; if it cannot be, the candidate must be informed in writing before the deadline expires, with a revised date that does not exceed a further 15 calendar days.

The reviewer must be a named, qualified consultant who has not previously been involved in the automated shortlisting decision for that candidate. They must read the candidate's original application documents in full. Where the original ATS ranking or a ChatGPT summary influenced an earlier decision, the reviewer must set that output aside and form an independent view. The reviewer's identity, the date of review and the conclusion reached must all be recorded as set out in Section 7.

No automated tool may be used as the primary basis for the human-review decision. The reviewer may use Microsoft 365 Copilot or the CRM to retrieve documents, but the assessment itself must be their own.

Where Marchwood Talent fails to respond within the applicable deadline, the candidate has a right to complain to the ICO. Marchwood Talent's complaints procedure (required to be operational from 19 June 2026) must include the ICO's contact details and the candidate's right to lodge a complaint without first exhausting Marchwood Talent's internal process.

7. Recording the Outcome of a Human Review

Every human review conducted under this document must be recorded in Marchwood Talent's ATS or CRM at the time it is completed, not retrospectively. The record must contain the following fields as a minimum: candidate name and unique reference; date the request was received; name and role of the reviewer; date the review was completed; the original automated outcome (for example, the ATS rank or ranking band, or the fact that a ChatGPT summary was used); the reviewer's independent assessment in at least two or three sentences explaining the basis for their conclusion; the final outcome communicated to the candidate; and the date and method by which the outcome was communicated.

Where the reviewer's conclusion differs from the automated outcome — for example, where the ATS excluded a candidate but the consultant considers them suitable — the record must also note what action was taken as a result (for example, candidate added to shortlist, presented to client, or placed).

These records must be retained for a minimum of six years from the date of the review, given that employment-related disputes can arise well after a placement has concluded. Records containing health declarations or criminal record data must be stored in access-controlled folders with a log of who has viewed them.

Aggregate review data — the number of requests received, outcomes overturned, and time to respond — must be collated quarterly by the designated compliance contact and reviewed by Marchwood Talent's senior leadership. This is the primary mechanism by which Marchwood Talent will detect and address systematic bias in its ATS or AI tools, as required by the Equality Act 2010 and the ICO's AI auditing framework. If the data shows a pattern of the ATS excluding candidates sharing a protected characteristic, Marchwood Talent must suspend automated shortlisting for the affected role type until the cause is identified and remedied.

8. Where Notices Appear and Proof of Delivery

Notices must appear in four locations to satisfy the transparency and accountability requirements of UK GDPR Articles 13, 14 and 22, and the ICO's AI auditing framework.

First, the ATS Shortlisting Notice (Section 3) must appear on the application form itself, as a distinct, clearly labelled section immediately before the submit button. It must not be embedded within the privacy policy or accessible only via a hyperlink. If the ATS does not support inline notice text, the form must include a mandatory acknowledgement tick-box referencing the notice, and the notice must appear on the immediately preceding page.

Second, both notices (Sections 3 and 4) must appear in Marchwood Talent's candidate privacy notice, which must be made available at first contact and again at the point a candidate's data is entered into the ATS.

Third, the ChatGPT Notice (Section 4) must be delivered by email to the candidate before their CV is pasted into any AI tool. The sending consultant must record the email send in the ATS candidate record at the time of sending.

Fourth, where Marchwood Talent operates a candidate portal or sends an automated acknowledgement email on receipt of an application, both notices must appear in that communication.

Proof of delivery is established as follows: for the application-form notice, the ATS submission timestamp is the record; for the email notice, the sent-item in the consultant's email client together with the ATS log entry; for the privacy notice, a version-controlled document with a publication date. Marchwood Talent must not rely on oral evidence alone to demonstrate that a notice was given. Where proof cannot be produced, the ICO will treat the notice as not having been given.

9. Shadow AI and Unapproved Tools

Marchwood Talent has declared that no policy is currently in place and no record exists of which tools are approved. Until a formal approved-tools register is established, every AI tool used by any consultant to process candidate data — including free or personal accounts of ChatGPT, any browser-based AI extension, or any AI feature activated within an existing platform — must be treated as in scope for this document's notice and recording requirements.

From the date this document is adopted, consultants must not use any AI tool to process candidate personal data unless that tool appears on Marchwood Talent's approved list and a data processing agreement is in place with the provider. A tool that generates a decision or recommendation about an individual, however incidentally, is a tool in scope. This includes AI drafting assistants used to write rejection emails where the content of the email is itself influenced by an AI assessment of the candidate.

Where a consultant is found to have used an unapproved tool, the candidate affected must be notified using the ChatGPT Notice wording in Section 4, adapted to name the actual tool used, and offered a human review under Section 6 regardless of the original outcome. The incident must be recorded and reviewed by the compliance contact within five working days.

This requirement directly addresses the Shadow AI risk identified by Marchwood Talent and is consistent with the ICO's published position that a controller cannot escape accountability for processing carried out by employees using personal accounts on third-party AI platforms.

Data Subject Rights Procedures for AI-Processed Data

How you answer an access, correction or deletion request when the data has passed through an AI system.

1. Purpose and Scope

This procedure governs how Marchwood Talent Limited ('Marchwood Talent') responds to data subject rights requests where the personal data concerned has been processed by, or passed through, an AI system. It applies to all AI tools in current use: the applicant tracking system ('ATS') that automatically ranks and shortlists candidates, ChatGPT / OpenAI (used by consultants to summarise CVs), Microsoft 365 Copilot, AI-enabled HR or recruitment systems, and AI-powered CRM or sales tools.

Marchwood Talent operates as a recruitment business placing candidates into financial services and healthcare. Candidate data routinely includes special-category information — specifically health declarations and criminal record data — which attracts heightened obligations under UK GDPR Articles 9 and 10. This procedure must be followed whenever a rights request involves data that has been input into, ranked by, summarised by, or otherwise touched by any of those tools. It sits alongside Marchwood Talent's broader data protection framework and should be read in conjunction with the AI Tool Register and the Data Protection Impact Assessments maintained for each AI system.

2. Rights, Statutory Deadlines and Internal Owners

Six rights are routinely engaged when personal data has passed through an AI system. Each carries a mandatory deadline under UK GDPR and must be assigned a named internal owner.

Right of Access (UK GDPR Article 15). A data subject may request confirmation that their data is being processed and a copy of all personal data held, including data that has been input into or produced by any AI tool. The deadline is one calendar month from receipt of the request, extendable by a further two months where the request is complex or numerous, provided the data subject is notified within the first month. Internal owner: the Data Protection Lead (or, until that role is formally appointed, the most senior consultant in the operations function).

Right to Rectification (UK GDPR Article 16). Where a data subject believes that data held — including a CV summary generated by ChatGPT or a ranking score produced by the ATS — is inaccurate or incomplete, they may require correction. The one-month deadline applies. Internal owner: the Data Protection Lead, coordinating with the relevant consultant.

Right to Erasure (UK GDPR Article 17). A data subject may request deletion of their personal data, including data held in AI vendor systems. The one-month deadline applies. This right is subject to specific limitations set out in Section 7 of this document. Internal owner: Data Protection Lead.

Right to Restriction (UK GDPR Article 18). Where a data subject contests accuracy, objects to processing, or requires data for legal claims, processing may be restricted rather than erased. The one-month deadline applies. Internal owner: Data Protection Lead.

Right to Object (UK GDPR Article 21). A data subject may object to processing based on legitimate interests. Where AI-based profiling or automated ranking is the basis for processing, this right has direct force. The one-month deadline applies. Internal owner: Data Protection Lead, escalating to the relevant system vendor where necessary.

Right Not to Be Subject to a Solely Automated Decision with Legal or Similarly Significant Effect (UK GDPR Article 22, as amended by the Data (Use and Access) Act 2025, in force 5 February 2026). A data subject has the right to obtain human review of any decision taken solely by automated means that produces a legal or similarly significant effect. The right to request human review, to express a point of view, and to contest the decision must be honoured within one month. Internal owner: Senior Consultant (for the review itself) and Data Protection Lead (for the

procedural response).

All requests received by any member of staff — by email, telephone, post or verbally — must be forwarded to the Data Protection Lead within 24 hours of receipt. The clock starts on the day the request is received, not the day it is passed internally.

3. Locating Personal Data Held Inside or by an AI Vendor

When a data subject request is received, the Data Protection Lead must conduct a systematic search across every AI system in scope before the response is issued. This is not optional: a Subject Access Response that fails to account for AI-held data is non-compliant with UK GDPR Article 15.

For the ATS, the Data Protection Lead must retrieve: the original CV and application data ingested by the system; any ranking score, shortlisting decision, or flag produced by the automated ranking engine; any notes or tags appended by the system; and any data retained in audit logs. Access credentials and search procedures for the ATS must be documented in the AI Tool Register. If the ATS vendor processes data on Marchwood Talent's behalf under a data processing agreement, the agreement must oblige the vendor to assist with rights requests within a timescale that allows Marchwood Talent to meet its own statutory deadline.

For ChatGPT / OpenAI, consultants have been pasting CVs — which include health and criminal record declarations — into the tool. OpenAI does not currently guarantee retrieval of specific inputs submitted via standard ChatGPT sessions, and inputs may be retained and used in model training unless the relevant data-sharing settings have been disabled. The Data Protection Lead must confirm, via the account settings active at the time of processing, whether data retention was enabled. If it was, a deletion request must be submitted to OpenAI through its privacy request portal, and the outcome must be recorded in the request log. The limitation on guaranteed retrieval must be disclosed to the data subject if a full copy of AI-processed data cannot be provided.

For Microsoft 365 Copilot, data inputs are processed within the Microsoft 365 tenant and are subject to the data processing terms in the Microsoft Customer Agreement. The Data Protection Lead must search Copilot interaction history and any outputs saved to SharePoint, Teams or Outlook. Microsoft's compliance tools, including the Microsoft Purview portal, should be used to locate relevant data.

For AI-enabled HR systems and AI-powered CRM tools, each vendor's data retrieval procedure must be documented in the AI Tool Register. The Data Protection Lead must submit a retrieval request to each vendor using the documented procedure and record the vendor's response and the data returned.

Where a vendor is unable to confirm whether a data subject's data has been retained or trained on, that uncertainty must be disclosed to the data subject in plain terms and recorded in the request log.

4. Explaining an Automated Decision in Terms a Person Understands

Where a data subject's application has been processed by the ATS automated ranking and shortlisting engine, Marchwood Talent is required by UK GDPR Article 22 and the ICO's AI Auditing Framework to provide meaningful information about the logic involved in any automated decision that produces a legal or similarly significant effect. A candidate being shortlisted or rejected by the ATS before any consultant reviews their application is likely to meet that threshold.

The explanation provided to the data subject must cover: the fact that an automated system was used; what data the system considered (for example, work history, qualifications, keywords); the general logic or criteria the system applied to produce a ranking or shortlisting outcome; the significance of that outcome for the data subject (for example, whether it determined whether a consultant reviewed their application at all); and what the data subject can do next, including their right to request human review.

The explanation must not use technical jargon, model names, or vendor descriptions that a candidate without technical knowledge could not understand. It must not be so vague as to be meaningless — a statement that 'an AI system reviewed your application' without further detail does not satisfy Article 22(3) or the ICO's expectations.

The Data Protection Lead, working with the relevant ATS vendor, must prepare a standing explanation template for the ATS ranking process. That template must be reviewed and updated whenever the ATS vendor changes the model, criteria, or weighting used. The explanation must be included in every Article 22 response and in every Subject Access Response where the ATS produced an output relating to the data subject.

5. The Right to Object and the Right to Human Review

Under UK GDPR Article 22(1) and the amended provisions brought into force by the Data (Use and Access) Act 2025 on 5 February 2026, Marchwood Talent may not make a decision based solely on automated processing — including profiling — that produces a legal or similarly significant effect on a data subject, unless at least one of the statutory exceptions applies. Shortlisting or rejecting a candidate using the ATS ranking engine without any consultant review before the decision is acted upon is a solely automated decision within the meaning of Article 22. The processing of special-category data (health and criminal record declarations) by an automated system engages the additional safeguard in Article 22(4): such processing requires either explicit consent or processing necessary for reasons of substantial public interest, under a domestic legal basis that also provides suitable measures to safeguard the data subject's rights.

Where a data subject objects to a decision produced or influenced by the ATS, or requests human review, the following steps apply. First, the Data Protection Lead acknowledges the objection or request in writing within five working days and confirms that automated processing has been paused or that the automated outcome will not be acted upon pending review. Second, a Senior Consultant who was not involved in the original ATS process must review the candidate's application manually, without reference to the ATS ranking score, within the one-month statutory period. Third, the Senior Consultant records their independent assessment in writing, including the reasons for the outcome reached. Fourth, the Data Protection Lead communicates the outcome of the human review to the data subject in writing, including the reasons for the decision and the data subject's right to complain to the ICO if they remain dissatisfied.

A data subject also has the right under Article 21 to object to processing based on legitimate interests at any time. Where such an objection is received, Marchwood Talent must cease AI-based processing of that individual's data unless it can demonstrate compelling legitimate grounds that override the individual's interests, rights and freedoms, or unless processing is necessary for the establishment, exercise or defence of legal claims.

6. Deletion Where a Vendor May Have Retained or Trained on Input Data

A right to erasure request under UK GDPR Article 17 does not end with deleting data from Marchwood Talent's own systems. Where personal data has been submitted to an AI vendor, Marchwood Talent must take reasonable steps to procure deletion from that vendor's systems and must document the outcome.

For the ATS, the data processing agreement must include an obligation on the vendor to delete or return all personal data on instruction and to confirm deletion in writing. The Data Protection Lead must submit a deletion instruction to the ATS vendor within five working days of receiving the data subject's erasure request and must record the vendor's written confirmation in the request log.

For ChatGPT / OpenAI, the position is more complex. OpenAI's standard terms for ChatGPT permit retention of inputs for safety and model improvement purposes unless the relevant setting has been disabled. If the setting was not disabled at the time a consultant pasted a candidate's CV into ChatGPT — which is the current position given the absence of any approved tool policy at Marchwood Talent — there is a material risk that the data has been retained and may have been used in model training. Marchwood Talent must submit a privacy deletion request to OpenAI through its official privacy request mechanism. If OpenAI confirms deletion, the confirmation must be recorded. If OpenAI cannot confirm deletion, or confirms that data was used in training and cannot be extracted, the Data Protection Lead must record this outcome and disclose it to the data subject in plain terms, explaining that the limitation arises from the vendor's technical architecture and that Marchwood Talent has taken all available steps to procure deletion. This situation also constitutes a compliance failure that must be recorded in the organisational risk register, because the submission of special-category data to ChatGPT without a data

processing agreement and without disabled retention settings was not compliant with UK GDPR from the outset.

For Microsoft 365 Copilot, deletion of Copilot-generated outputs and interaction data can be managed through the Microsoft Purview compliance portal and through standard data subject request tooling within the Microsoft 365 admin centre. The Data Protection Lead must use these tools and retain a record of the deletion actions taken.

For all other AI vendors, the deletion procedure documented in the AI Tool Register must be followed, and vendor confirmation must be obtained and logged.

7. Refusal Grounds and Recording a Refusal

Marchwood Talent may refuse a data subject rights request, or refuse to take a specific action within a request, only where a statutory ground applies. No refusal may be issued on the basis of inconvenience, commercial sensitivity, or the difficulty of retrieving data from an AI vendor.

The grounds available under UK GDPR that are most likely to arise in Marchwood Talent's context are as follows. For access requests, manifestly unfounded or excessive requests may be refused or subject to a reasonable fee (Article 12(5)); however, the threshold for 'manifestly unfounded or excessive' is high and must not be applied routinely. For erasure requests, refusal is permissible where retention is necessary for compliance with a legal obligation (Article 17(3)(b)), for the establishment, exercise or defence of legal claims (Article 17(3)(e)), or for archiving, research or statistical purposes subject to the conditions in Article 17(3)(d). In the recruitment context, Marchwood Talent may be required to retain certain records for employment or regulatory purposes, but this must be assessed individually for each request. For requests relating to automated decisions, Marchwood Talent cannot refuse a request for human review on the ground that the ATS produces more accurate results than a human reviewer; accuracy is not a statutory ground for refusing the right under Article 22.

Every refusal — whether in whole or in part — must be recorded in the request log using the template in Section 8. The record must state: the specific statutory ground relied upon; the facts that bring the request within that ground; the name of the person who made the refusal decision; and the date. The data subject must be informed of the refusal in writing, given the specific ground relied upon in plain language, told of their right to complain to the ICO, and told of their right to seek a judicial remedy under Article 79. The refusal response must be issued within the statutory one-month period; it is not permissible to allow the deadline to pass without issuing either a substantive response or a refusal.

8. Request Log Template

All data subject rights requests involving AI-processed data must be recorded in the Marchwood Talent Data Subject Rights Log. A separate row must be created for each request. The log must be maintained by the Data Protection Lead and retained for a minimum of three years. The following fields are mandatory for every entry.

Request reference number. A unique sequential identifier assigned at the point the request is received.

Date request received. The calendar date on which the request was received by any member of staff, which is the date from which the statutory deadline runs.

Date forwarded to Data Protection Lead. Must be within 24 hours of receipt.

Data subject name and contact details. As provided by the data subject.

Nature of request. Specify the right(s) invoked: access; rectification; erasure; restriction; objection; human review of automated decision; or a combination.

AI systems involved. List every AI tool in scope for this request, drawn from: ATS; ChatGPT / OpenAI; Microsoft 365 Copilot; HR or recruitment AI system; CRM AI tool.

Special-category or criminal record data involved. Yes or No. If yes, specify the category (health declaration; criminal record data; other).

Vendor data retrieval actions. For each AI vendor: date retrieval request submitted; date response received; summary of data retrieved or confirmation that no data held.

Vendor deletion actions (erasure requests only). For each AI vendor: date deletion instruction submitted; date confirmation received; outcome (confirmed deleted; unable to confirm; data used in training — cannot extract).

Automated decision explanation provided. Yes / Not applicable. If yes, date provided and version of explanation template used.

Human review conducted (Article 22 requests). Yes / Not applicable. If yes, name of Senior Consultant who conducted the review and date of review.

Statutory deadline. One calendar month from date received, or extended deadline if extension invoked (state extension invoked date and new deadline).

Response issued date. The calendar date on which the substantive response was sent to the data subject.

Outcome. Complied in full; partially complied (specify what was withheld and the ground); refused (specify ground).

Refusal ground (if applicable). The specific statutory provision relied upon, the facts engaged, and the name of the decision-maker.

Data subject notified of right to complain to ICO. Yes or No.

Complaint received from data subject following response. Yes or No. If yes, cross-reference to the complaints procedure log. Note: under the Data (Use and Access) Act 2025 provisions in force from 19 June 2026, Marchwood Talent is required to operate a complaints procedure and respond to data protection complaints within set time limits. Every complaint received must be logged and handled in accordance with that procedure.

Notes. Any additional information relevant to the handling of the request.

9. Applicable Law and Regulatory Framework

This procedure is grounded in the following legal instruments as they apply in the United Kingdom. UK GDPR Articles 12 to 22 establish the data subject rights framework, including access, rectification, erasure, restriction, objection, and rights relating to automated decision-making. Article 22 specifically governs solely automated decisions with legal or similarly significant effects; Article 22(4) imposes additional safeguards where special-category data is processed by automated means. Articles 9 and 10 govern the processing of health data and criminal record data respectively, both of which Marchwood Talent processes in the recruitment context. The Data (Use and Access) Act 2025 amended the UK automated decision-making framework; the relevant Part 5 provisions came into force on 5 February 2026, and the duty to operate a complaints procedure and respond within set time limits came into force on 19 June 2026. The ICO AI Auditing Framework sets out the ICO's expectations for transparency, explainability and accountability in AI systems, including those used in recruitment; Marchwood Talent's use of the ATS falls directly within the scope of the ICO's November 2024 audit outcomes on AI in recruitment. The UK Equality Act 2010 is engaged where an automated ranking or shortlisting system produces outcomes that disadvantage candidates sharing a protected characteristic; this procedure must be operated in a way that does not obstruct a data subject from obtaining information relevant to an equality complaint. The maximum ICO fine for a serious UK GDPR infringement is £17.5 million or 4% of global annual turnover, whichever is higher; the turnover-based limb cannot be calculated without Marchwood Talent's audited global turnover figures.

This procedure takes effect from the date shown on the compliance pack cover sheet and must be reviewed whenever a new AI tool is adopted, whenever a vendor changes its data retention or training practices, or whenever there is a material change in applicable law or ICO guidance.

Sector-Specific Obligations Review

The rules that apply because of the sector you are in, on top of the general AI and data regime.

Regulators with Jurisdiction over Marchwood Talent

Marchwood Talent operates in the recruitment sector, placing candidates permanently and on contract into financial services and healthcare. This means the business sits within the oversight reach of several regulators simultaneously, not just the Information Commissioner's Office.

The Financial Conduct Authority (FCA) has jurisdiction over conduct affecting FCA-authorised firms and, increasingly, over the third-party suppliers those firms rely upon. Where Marchwood Talent supplies candidates to FCA-regulated clients, the FCA's operational resilience and third-party risk frameworks require those clients to scrutinise how Marchwood conducts its processes — including AI-assisted screening. In practice, this creates downstream contractual and reputational pressure on Marchwood to meet standards its clients are themselves required to uphold.

The Medicines and Healthcare products Regulatory Agency (MHRA) and NHS commissioning bodies govern the healthcare sector into which Marchwood places candidates. Roles in clinical or regulated healthcare settings carry statutory fit-and-proper-person requirements and, in many cases, mandatory disclosure of health conditions or criminal convictions. AI-assisted screening of candidates for such roles therefore intersects directly with regulatory requirements that sit outside data protection law.

The Equality and Human Rights Commission (EHRC) enforces the Equality Act 2010 and has published guidance specifically on algorithmic decision-making and discrimination. Because Marchwood's applicant tracking system (ATS) ranks and shortlists candidates automatically before a consultant reviews them, the EHRC is a live enforcement body, not a background concern.

The ICO remains the primary regulator for data protection and automated decision-making obligations, including under UK GDPR Article 22 and the Data (Use and Access) Act 2025. The ICO published the outcomes of an audit of AI tools in recruitment in November 2024, making recruitment a named priority sector. Marchwood should treat ICO guidance in this area as directly applicable to its current practices.

Sector Rules Bearing on AI Use

Several named sector-specific rules apply to Marchwood Talent's AI deployments, each with distinct requirements.

The Equality Act 2010 prohibits direct and indirect discrimination on the basis of protected characteristics including race, sex, age, disability, religion, and pregnancy. Where Marchwood's ATS automatically ranks and shortlists candidates, any ranking algorithm that produces outcomes with a disparate adverse impact on a protected group constitutes indirect discrimination unless Marchwood can objectively justify the criterion applied. The burden of establishing justification rests with Marchwood. This is not a future risk — automatic ranking is already in operation and no bias audit has been conducted.

UK GDPR Article 22 gives data subjects the right not to be subject to a decision based solely on automated processing that produces a legal or similarly significant effect concerning them. Candidate shortlisting — determining who is presented to a client and who is rejected — is a decision with significant effect on a candidate's ability to obtain employment. Where the ATS makes that determination without meaningful human review, Article 22 is engaged. Marchwood must be able to demonstrate either that a lawful basis exception applies or that a consultant exercises genuine, substantive review before any decision takes effect. Pasting CVs into ChatGPT without a data processing agreement does not constitute meaningful human review for this purpose; it is a separate and additional compliance failure.

The Data (Use and Access) Act 2025, most of whose Part 5 data protection provisions came into force on 5 February 2026, has amended the UK framework for solely automated decisions. It introduces wider lawful bases for such decisions and associated safeguards. The duty on controllers to operate a complaints procedure for data protection complaints, with responses required within set time limits, came into force on 19 June 2026. Marchwood has no policy in place and no complaints procedure, meaning it is already in breach of this provision as of the date of this review.

The ICO's AI Auditing Framework sets out expectations for organisations using AI in high-risk contexts. Recruitment is identified as a high-risk context. The framework requires documented accountability, bias testing, transparency to data subjects, and human oversight mechanisms. Marchwood currently meets none of these requirements for its ATS or its ChatGPT use.

FCA Sourcebook provisions — in particular, the Senior Managers and Certification Regime (SM&CR;) requirements applicable to Marchwood's financial services clients — create indirect obligations. Those clients must ensure that critical third-party suppliers, including recruitment firms screening candidates for regulated roles, operate processes that do not create regulatory risk. Where Marchwood's AI screening introduces bias or data protection failures into hiring for FCA-regulated roles, Marchwood's clients face regulatory exposure, and Marchwood faces contractual liability and loss of client relationships.

For healthcare placements, the Care Quality Commission (CQC) regulates providers who use Marchwood's candidates. CQC fit-and-proper-person requirements under Regulation 5 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 mean that healthcare clients must be able to confirm the integrity of the candidate vetting process. An AI system that has not been validated for bias or accuracy in assessing candidates for healthcare roles undermines the evidential basis for those clients' compliance.

Where Sector Rules Are Stricter Than the General Regime

The general AI and data protection regime imposes baseline obligations, but Marchwood's sector operations intensify several of these in ways that the general rules alone do not capture.

On special category data, UK GDPR Article 9 requires explicit consent or another specific Article 9(2) condition for processing data concerning health, and Schedule 1 of the Data Protection Act 2018 governs processing of criminal conviction data under Article 10 UK GDPR. Marchwood's candidate data for healthcare placements includes health declarations, and data for both financial services and healthcare placements includes criminal record information. The general regime requires a lawful basis plus an Article 9 condition. The sector context adds a further layer: healthcare clients and financial services clients are themselves subject to regulatory duties requiring that such data be handled with specific procedural rigour. Where Marchwood uses ChatGPT or its ATS to process health or criminal record data, it must hold an explicit lawful basis for each processing activity, have Data Processing Agreements in place with each AI tool provider, and be able to demonstrate that special category data is not transmitted to tools — such as the consumer version of ChatGPT — that are not configured as data processors. None of this is currently documented.

On transparency, the general UK GDPR Articles 13 and 14 require candidates to be informed of automated decision-making. The sector expectation goes further: the ICO's November 2024 recruitment audit outcomes specifically flagged that candidates must be told not only that automated processing occurs, but what criteria are applied and what the consequences are. Candidates for financial services and healthcare roles — where criminal and health data is actively assessed — have a heightened legitimate expectation of transparency that the standard privacy notice minimum does not satisfy.

On accuracy and bias, the general regime requires that personal data be accurate (Article 5(1)(d) UK GDPR). In recruitment AI, accuracy has an additional dimension: an inaccurate or biased ranking directly causes a candidate to be excluded from employment opportunities. For healthcare roles this carries patient safety implications. For financial services roles it affects FCA-regulated firms' ability to conduct fit-and-proper assessments on the basis of a pool that has already been distorted by algorithmic bias. These downstream harms elevate the accuracy obligation from an administrative requirement to one with direct sector regulatory consequences for Marchwood's

clients and, by extension, reputational and contractual consequences for Marchwood.

Professional and Indemnity Obligations Engaged by AI Use

Marchwood Talent's professional obligations and insurance position are materially affected by its current AI practices.

Recruitment consultants owe a duty of care to both the candidate and the client. Where a consultant relies on an ATS shortlist without substantive independent review, and the shortlist contains biased or inaccurate rankings, the consultant may be found to have delegated professional judgement to an automated system. This is particularly acute for financial services and healthcare placements, where a poor or negligent placement can result in regulatory sanctions for the client, patient harm, or financial loss. Courts have shown willingness — as illustrated by the May 2026 Pinsent Masons case — to criticise professionals who rely on AI outputs without adequate verification. Marchwood's consultants summarising CVs using ChatGPT without verification protocols are engaged in precisely this risk behaviour.

Professional indemnity (PI) insurance policies for recruitment businesses typically contain exclusions or conditions relating to automated systems, undisclosed data processing activities, and regulatory non-compliance. Marchwood currently has no record of which tools are approved and no policy governing AI use. Where a claim arises from a biased shortlist or a data breach caused by pasting special category candidate data into ChatGPT without a data processing agreement, Marchwood's insurer may decline cover on the basis that the activity was either undisclosed or in breach of a regulatory requirement that the policy assumed would be met. Marchwood should notify its PI insurer of its AI tool usage and confirm the scope of cover before any claim situation arises.

Contracts with financial services and healthcare clients are likely to contain representations about data handling standards, confidentiality, and regulatory compliance. Marchwood's current practice of processing candidate health and criminal record data through unapproved AI tools — including the consumer version of ChatGPT which does not carry the data processor assurances of an enterprise agreement — constitutes a potential breach of those contractual representations. Discovery of this practice by a client could trigger contract termination and claims for breach, independently of any regulatory enforcement.

Reporting and Approval Duties Owed to Sector Regulators

Marchwood Talent carries specific reporting and approval duties arising from its sector context, over and above the general obligation to report personal data breaches to the ICO within 72 hours under UK GDPR Article 33.

Where a data breach involves candidate health or criminal record data relating to individuals placed or being considered for placement in healthcare settings, Marchwood must assess whether the breach requires notification to affected data subjects under Article 34 UK GDPR, where the breach is likely to result in a high risk to their rights and freedoms. Given the sensitivity of health and criminal record data, the threshold for high risk is readily met. Marchwood has no breach response procedure in place and no record of which tools hold which categories of data — making breach identification and 72-hour notification practically impossible in its current state.

The Data (Use and Access) Act 2025 requires Marchwood, as a controller operating automated decision-making processes, to operate a complaints procedure for data protection complaints and to respond within the set time limits. This duty came into force on 19 June 2026. Marchwood has no such procedure. Any candidate who complains about ATS-driven shortlisting decisions is entitled to a substantive response within the prescribed period; failure to provide one is a breach of a current statutory duty, not a future risk.

Although Marchwood is not itself an FCA-authorised firm, the FCA's expectations flow through its regulated clients. Where those clients are required by the FCA's Operational Resilience rules (PS21/3) to assess and manage risks posed by material third parties, they may impose contractual audit rights over Marchwood's AI practices. Marchwood should anticipate client due diligence requests on its AI tools, data processing arrangements, and bias testing, and treat the absence of documentation as a commercial risk that is already live.

For healthcare sector placements, where Marchwood processes sensitive data under statutory disclosure schemes — including Disclosure and Barring Service (DBS) checks — any AI tool that processes, stores, or summarises that data must be assessed against the DBS Code of Practice. Using ChatGPT to summarise CVs containing DBS disclosure information is a direct violation of the requirement that such information be handled only through secure, defined processes. There is no approval by the DBS or any other body that would cover the current practice, and no such approval is available for consumer AI tools. Marchwood must cease this specific practice immediately and document the cessation.

AI Risk Register

The ongoing record of AI risks, their owners and their mitigations. A live document — review it on the cadence stated at the foot.

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-01	Candidate CV data (incl. health and criminal record declarations) pasted into ChatGPT is processed on OpenAI servers outside Marchwood's control, risking data leakage.	ChatGPT / OpenAI — consultant CV summarisation	High	Critical	Critical	Ban CV pasting into ChatGPT immediately. Issue written instruction to all staff. Implement approved summarisation tool with a Data Processing Agreement. Log compliance.	Head of Operations	Medium	11 Nov 2026
RR-02	Special-category data (health declarations, criminal record checks) processed via AI without an explicit legal basis breaches UK GDPR Art 9 and Art 10.	ChatGPT / OpenAI; ATS automated ranking	High	Critical	Critical	Document lawful basis and explicit consent or Schedule 1 DPA 2018 condition for each special-category field before any AI processes it. Record in ROPA.	Data Protection Lead	Medium	11 Nov 2026
Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-03	ATS automatically ranks and shortlists candidates before a consultant reviews	ATS automated candidate ranking and shortlisting	High	Critical	Critical	Comply with UK GDPR Art 22 and DUAA Part 5 (in force 5 Feb	Head of Recruitment	Medium	11 Feb 2027

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	them, constituting solely automated decision-making with legal or similarly significant effect.					2026): document lawful basis, implement right to human review, notify candidates, log decisions.			
RR-04	ATS ranking model may embed historical bias, producing discriminatory shortlists that unlawfully disadvantage protected-characteristic groups in financial services and healthcare roles.	ATS automated candidate ranking and shortlisting	High	Critical	Critical	Commission bias audit of ATS algorithm. Test outputs by protected characteristic (Equality Act 2010 ss.4, 19). Document results. Require vendor to provide bias-testing evidence.	Head of Recruitment	High	11 Feb 2027
RR-05	ChatGPT CV summaries may omit, distort or hallucinate candidate information; consultants relying on inaccurate summaries make flawed placement decisions.	ChatGPT / OpenAI — CV summarisation	High	High	Critical	Until RR-01 ban is lifted, mandate consultant verification of every AI summary against original CV. Record verification step in ATS audit trail.	Recruitment Manager	Medium	11 Nov 2026

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-06	Microsoft 365 Copilot may surface candidate or client personal data from emails and documents to unauthorised users via AI-generated responses or summaries.	Microsoft 365 Copilot	Medium	High	High	Audit M365 permission model before enabling Copilot. Restrict Copilot access to roles that need it. Confirm Microsoft DPA is in place. Review Copilot tenant settings.	IT Manager	Medium	11 Feb 2027
RR-07	Copilot-generated marketing content may inadvertently include personal data or make inaccurate claims about Marchwood's services, creating regulatory and reputational exposure.	Microsoft 365 Copilot — marketing content	Medium	Medium	High	All Copilot-drafted external content reviewed and approved by a named person before publication. Maintain review log. Include AI-content disclaimer in internal style guide.	Marketing Lead	Low	11 Feb 2027
Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-08	Employees using AI tools not approved by Marchwood (shadow AI) are processing candidate and client data on unvetted	Any unapproved AI tool used by staff	High	Critical	Critical	Publish an Approved AI Tools List immediately. Prohibit non-listed tools via a acceptable-use policy. Technical	Head of Operations	Medium	11 Nov 2026

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	platforms with no DPA, no oversight and no audit trail.					controls (web filtering) to block known AI platforms not on list.			
RR-09	AI-powered CRM analyses candidate and client data for sales intelligence; purpose may exceed original consent scope, breaching UK GDPR Arts 5(1)(b) and 6.	AI-powered CRM / sales tools	Medium	High	High	Map CRM AI features. Confirm each use is compatible with original collection purpose or obtain fresh consent. Update privacy notices. Record in ROPA.	Data Protection Lead	Medium	11 Feb 2027
RR-10	AI in HR or recruitment performance systems may evaluate consultant performance using opaque metrics, creating unfair employment decisions and Art 22 exposure.	AI in HR / recruitment performance management	Medium	High	High	Identify any solely automated HR decisions. Apply DUAA Part 5 safeguards. Ensure human sign-off on all performance outcomes. Inform affected employees per Art 13/14.	HR Manager	Medium	11 Feb 2027
Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-11	ATS or CRM vendor suffers outage, data breach or	ATS; AI-powered CRM	Medium	High	High	Review vendor contracts for SLAs, breach notification obligations	Head of Operations	Medium	11 Aug 2027

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	insolvency, causing loss of candidate data and disruption to live placements in regulated sectors.					and data return/deletion on termination. Maintain offline backups. Include vendor risk in annual review.			
RR-12	No Data Processing Agreements in place with AI vendors, meaning Marchwood cannot demonstrate processor compliance under UK GDPR Art 28, exposing it to ICO enforcement.	All AI tools processing personal data	High	High	Critical	Execute Art 28-compliant DPAs with OpenAI, Microsoft, ATS vendor and CRM vendor before further processing. File signed copies centrally. Review on vendor contract renewal.	Data Protection Lead	Medium	11 Nov 2026
RR-13	No DPIA has been conducted for high-risk AI processing (automated ranking of candidates, special-category data), breaching UK GDPR Art 35 and ICO AI Auditing Framework expectations.	ATS automated ranking; ChatGPT; HR AI systems	High	High	Critical	Conduct DPIAs for all high-risk AI processes. Use ICO DPIA template. Consult ICO if residual risk remains high after mitigation. File completed DPIAs internally.	Data Protection Lead	Medium	11 Nov 2026

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-14	Regulatory change — DUAA Part 5 complaint-handling duty (in force 19 Jun 2026) requires a documented complaints procedure and timely responses ; Marchwood has no such procedure.	All AI tools involving automated decisions about people	High	High	Critical	Draft and publish an AI-related data protection complaints procedure. Assign a named handler. Log all complaints and responses. Comply with DUAA timescale requirements.	Data Protection Lead	Medium	11 Nov 2026
RR-15	ICO enforcement action or fine following audit — maximum £17.5m or 4% of global annual turnover — triggered by any of the compliance gaps documented in this register.	All AI tools and processes	High	Critical	Critical	Prioritise RR-01, RR-02, RR-03, RR-12 and RR-13 for immediate remediation. Maintain evidence of mitigations taken. Appoint or designate a DPO or data lead formally.	Managing Director	Medium	11 Nov 2026
Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
RR-16	Data analysis outputs from AI/BI tools may reflect biased training data, producing misleading market or candidate-pool	AI-powered CRM / data analysis and BI tools	Medium	Medium	Medium	Document data sources feeding BI/ AI. Require human analyst sign-off before insights are used in strategy.	Head of Operations	Low	11 Aug 2027

Risk ID	Risk	Tool or Process	Likelihood	Impact	Inherent Rating	Mitigation	Owner	Residual Rating	Review Date
	insights that inform discriminatory business decisions.					Flag where protected-characteristic proxies may be present.			

RATING SCALE DEFINITIONS — Two scorers must apply these definitions to reach the same rating.

LIKELIHOOD: Low = unlikely in the next 12 months given current controls; Medium = plausible within 12 months; High = likely within 12 months or already occurring.

IMPACT: Low = minor operational disruption, no regulatory or legal consequence; Medium = material operational impact or possible regulatory interest, recoverable; High = significant financial loss, regulatory investigation, or reputational damage; Critical = ICO enforcement or fine, litigation, placement in regulated sector halted, or serious harm to a data subject.

INHERENT RATING (before mitigation): Low × Low = Low; Medium × Medium = Medium; High × High = Critical. Mixed scores: use the higher of the two. Inherent rating = worst-case position with no controls applied.

RESIDUAL RATING (after mitigation): Re-score Likelihood and Impact assuming stated mitigations are fully implemented. Residual rating reflects the position Marchwood should reach once the register's actions are complete.

RATING MATRIX:

- Low / Low = Low
- Low / Medium = Low
- Medium / Medium = Medium
- Medium / High = High
- High / High = Critical
- Any Critical Impact = at least High, regardless of Likelihood

REGULATORY CONTEXT FOR THIS REGISTER

UK GDPR Art 22 and the Data (Use and Access) Act 2025 Part 5 (in force 5 February 2026) govern solely automated decisions with legal or similarly significant effect. The DUAA also introduced a duty to operate a complaints procedure for data protection matters (in force 19 June 2026). UK GDPR Arts 5, 6, 9, 10, 13, 14, 28 and 35 apply across the processing activities recorded here. The UK Equality Act 2010, including the public sector equality duty and the prohibition on indirect discrimination (s.19), applies to automated shortlisting affecting protected characteristics. The ICO AI Auditing Framework sets the practical standard the ICO uses when reviewing recruitment AI. Maximum ICO fine: £17.5 million or 4% of global annual turnover, whichever is higher; the turnover-based limb cannot be computed without Marchwood's annual turnover figures.

SPECIAL-CATEGORY AND CRIMINAL RECORD DATA NOTE

Health declarations and criminal record information processed in connection with financial services and healthcare placements are special-category data (UK GDPR Art 9) and criminal convictions data (Art 10 / DPA 2018 s.10 and Schedule 1). These attract the highest level of protection. No AI tool — including the ATS or ChatGPT — may process these data fields without an identified Schedule 1 DPA 2018 condition documented before processing begins.

OWNER DEFINITIONS

- Managing Director: accountable to the board; escalation point for Critical residual risks.
- Head of Operations: responsible for approved tool list, vendor contracts, DPA execution and shadow AI controls.
- Head of Recruitment: responsible for ATS configuration, consultant workflow and bias audit commissioning.
- Data Protection Lead: responsible for DPIAs, ROPA, Art 28 DPAs, complaints procedure and regulatory correspondence.
- IT Manager: responsible for M365 Copilot tenant settings, access controls and technical shadow-AI blocks.
- HR Manager: responsible for AI used in internal HR and consultant performance management.
- Recruitment Manager: responsible for day-to-day consultant compliance with CV-handling rules.

- Marketing Lead: responsible for AI-assisted content review and approval log.

REVIEW CADENCE

This register must be reviewed: (a) every six months as a minimum (next full review: 11 February 2027); (b) immediately on adoption of any new AI tool; (c) within 30 days of any material regulatory change (including ICO guidance, DUAA commencement instruments or FCA/MHRA sector guidance affecting recruitment into financial services or healthcare); and (d) following any data breach, complaint or ICO enquiry involving an AI tool. Risks rated Critical at residual level must be reviewed at the next monthly senior leadership meeting until downgraded. This document is version-controlled; each review must be dated, signed off by the Managing Director, and filed in the compliance record.

AI Incident Response Procedure

What happens in the first hour after an AI-related incident, and who does it. The regulator clock starts before anyone has decided who is in charge.

1. Purpose and Scope

This AI Incident Response Procedure sets out what Marchwood Talent must do, who must do it, and in what sequence, when an artificial intelligence system causes or contributes to an adverse event. It applies to every AI tool in use at Marchwood Talent, including the applicant tracking system (ATS) that automatically ranks and shortlists candidates, ChatGPT / OpenAI used by consultants to summarise CVs, Microsoft 365 Copilot, HR and recruitment system AI features, and AI-powered CRM or sales tools.

Because Marchwood Talent places candidates into financial services and healthcare, candidate data routinely includes criminal record disclosures and health declarations. These are special category data under UK GDPR and their exposure or misuse carries the highest regulatory consequences. The ICO's maximum fine is £17,500,000 or 4% of global annual turnover, whichever is higher; the turnover-based limb cannot be computed here without Marchwood Talent's figures, but the fixed maximum applies regardless of size.

This procedure is legally grounded in UK GDPR Articles 5, 22, 33, and 34; the Data (Use and Access) Act 2025 (Part 5 provisions in force from 5 February 2026, complaints procedure duty in force from 19 June 2026); the ICO AI Auditing Framework; and the UK Equality Act 2010. It is effective from 11 August 2026 and must be reviewed after any activation and at least annually.

2. What Counts as an AI Incident

An AI incident at Marchwood Talent is any event in which an AI tool produces, contributes to, or conceals an outcome that causes harm, creates regulatory exposure, or undermines the rights of a candidate, worker, client, or third party. The event need not be deliberate; a misconfiguration, a model hallucination, or an unforeseen interaction between tools is sufficient.

Examples specific to Marchwood Talent include: the ATS ranking or excluding a candidate in a way that correlates with a protected characteristic such as disability, race, sex, or age, in breach of the Equality Act 2010; a consultant pasting a CV containing health or criminal record information into ChatGPT, transmitting special category data to OpenAI's servers without a lawful basis or appropriate safeguard; Microsoft 365 Copilot surfacing one candidate's sensitive data to a user who has no legitimate need for it; the ATS making a shortlisting decision that the candidate can demonstrate they were never given a meaningful opportunity to challenge, engaging Article 22 UK GDPR on solely automated decisions with significant effect; an AI-powered CRM generating and sending client-facing content that is factually wrong or defamatory; discovery that consultants have been using an AI tool that is not on any approved list (shadow AI); a vendor notifying Marchwood Talent of a breach or vulnerability in an AI system that processes candidate data; and any AI output that a client in financial services or healthcare relies upon for a compliance-sensitive hiring decision that later proves flawed.

3. Severity Levels and Triggered Response

Marchwood Talent uses three severity levels. The level must be assigned within fifteen minutes of the incident being reported and may be escalated but not downgraded without written justification from the Data Protection Lead.

Level 1 — Critical. Applies where: special category data (health or criminal record information) has been or may have been exposed to an unauthorised party, including transmission to a third-party AI vendor without a valid legal basis; the ATS has produced shortlisting decisions that prima facie discriminate on a protected characteristic

across a cohort of candidates; a candidate has suffered a concrete adverse outcome (rejection, non-placement, reputational harm) attributable to an AI error; or a personal data breach involving AI-processed data has occurred or is suspected. Response: immediate containment and tool suspension within the first hour; Data Protection Lead and Managing Director notified within fifteen minutes; regulatory notification assessment begun immediately; affected individuals identified within two hours; vendor escalated within one hour; ICO notification decision made and actioned within the statutory window.

Level 2 — Significant. Applies where: an AI tool has produced an output that is materially inaccurate or misleading but has not yet reached a candidate or client; shadow AI use is confirmed involving personal data; the ATS has behaved anomalously but no confirmed discriminatory outcome exists; or a vendor has flagged a vulnerability not yet exploited. Response: tool suspended pending investigation; Data Protection Lead notified within one hour; investigation opened within four hours; regulatory notification assessed; vendor contacted within four hours.

Level 3 — Minor. Applies where: an AI tool produces a low-quality or incorrect output caught before use; a consultant reports a near-miss with no personal data involved; or a tool behaves unexpectedly with no data or rights impact. Response: incident logged in the AI Incident Register by end of business; no tool suspension required unless the Data Protection Lead directs otherwise; reviewed at next scheduled AI governance meeting.

4. First-Hour Actions: Contain, Preserve, Stop

The first hour is the period in which regulatory clocks start running and evidence is most at risk of being lost or overwritten. Every person at Marchwood Talent who identifies or suspects an AI incident must report it immediately to the Data Protection Lead (or their deputy if the Lead is unavailable) and must not attempt to resolve it independently, delete outputs, or notify candidates or clients without authorisation.

Contain. The person reporting must stop their own use of the affected tool immediately. The Data Protection Lead must assess within fifteen minutes whether the tool must be suspended organisation-wide. For a Level 1 incident, suspension is the default; the Lead must actively decide and document any exception. Where the ATS is involved, no further automated shortlisting decisions should be released to consultants or clients until the tool is cleared. Where ChatGPT or another external AI has received data, the Lead must assess whether a deletion request to the vendor is possible and appropriate.

Preserve evidence. Before any tool is reconfigured, updated, or accessed for remediation, the following must be captured and stored in a named, access-controlled folder: screenshots or exports of the AI output in question; the input data or prompt used; system logs or audit trails from the ATS or CRM; the identity of the consultant or system that triggered the action; timestamp of discovery; and any communications already sent to candidates or clients referencing the output. Preservation takes priority over remediation. Evidence must not be altered.

Stop the tool. The Data Protection Lead has authority to suspend any AI tool at Marchwood Talent without further approval for the duration of the investigation. Suspension means: consultants are instructed not to use the tool; automated processes feeding into or from the tool are paused; and the vendor is notified that the tool is under incident review. The Managing Director must be informed of any suspension within thirty minutes.

5. Named Roles and Deputies

Marchwood Talent must designate named individuals to each role before this procedure is activated. The following roles are defined; the business must insert the named person and their deputy in the live version of this document.

Data Protection Lead (insert name). Responsible for the overall incident response, regulatory notification decision, evidence preservation, and communication with the ICO. Has authority to suspend AI tools, instruct vendor escalation, and direct all staff actions during an incident. **Deputy** (insert name) assumes all powers if the Lead is unavailable.

Managing Director (insert name). Responsible for approving any public or client-facing communication about the incident, authorising expenditure required for remediation, and signing off the post-incident review report. **Deputy**

(insert name).

AI Tools Owner (insert name). Responsible for executing the technical suspension of tools, liaising with IT or system administrators, and coordinating vendor access. This person holds login credentials and vendor contact details for the ATS, ChatGPT business account, Microsoft 365 Copilot tenant administration, the HR system, and the CRM. Deputy (insert name).

Legal Adviser (insert name or firm). Consulted on the regulatory notification decision for Level 1 incidents and on any Equality Act 2010 exposure. Must be contactable within one hour for Level 1.

All role-holders must have a printed or offline copy of this procedure and the vendor contact sheet, because a cybersecurity incident may render internal systems inaccessible.

6. Regulator Notification Decision and Statutory Deadline

The statutory deadline under UK GDPR Article 33 is 72 hours from the point at which Marchwood Talent becomes aware of a personal data breach. Awareness is the moment any staff member, not just the Data Protection Lead, has sufficient information to establish that a breach is likely to have occurred. The clock does not start when the Lead is informed; it starts when the organisation first has that knowledge. This distinction is critical: a consultant who discovers at 9 a.m. that they pasted health data into an unsanctioned AI tool starts the clock at 9 a.m., regardless of when they report it internally.

The Data Protection Lead must make the notification decision within the first hour for any Level 1 incident. The test under Article 33 is whether the breach is likely to result in a risk to the rights and freedoms of natural persons. Given that Marchwood Talent processes special category data and places into sectors where criminal record and health information directly affects employability, the threshold will almost always be met for incidents involving that data. Notification to the ICO (report.ic.o.org.uk) is the default for Level 1 incidents; the Lead must document the reasoning if notification is withheld.

The Data (Use and Access) Act 2025, with its complaints procedure provisions in force from 19 June 2026, also requires Marchwood Talent to operate a procedure for responding to data protection complaints within defined time limits. Where an incident leads to a candidate complaint, that complaint must be logged, acknowledged, and processed under that procedure in parallel with the regulatory notification track.

If the incident raises concerns about the ATS's automated decisions under UK GDPR Article 22, the ICO AI Auditing Framework should be referenced in the notification to demonstrate that Marchwood Talent is applying a structured response. The ICO conducted a recruitment AI audit with published outcomes in November 2024; Marchwood Talent should be aware that the ICO has direct sector knowledge and will expect evidence of a systematic response, not an ad hoc one.

7. Notifying Affected Individuals

UK GDPR Article 34 requires Marchwood Talent to notify affected individuals directly, without undue delay, where a personal data breach is likely to result in a high risk to their rights and freedoms. The threshold for individual notification is higher than that for ICO notification: high risk, not merely risk. For Marchwood Talent, the following scenarios meet this threshold and require individual notification: health or criminal record data transmitted to an unauthorised AI system or third party; a candidate rejected or deprioritised by the ATS on grounds that correlate with a protected characteristic; a candidate's CV data exposed to another candidate, client, or unintended recipient via an AI tool; and any AI output about a specific individual that is materially false and has been communicated externally.

The Data Protection Lead must identify affected individuals within two hours of a Level 1 incident being declared. Notification must be written, in plain English, and must state: what data was involved; what happened; the likely consequences; and what steps Marchwood Talent is taking. It must not contain legal disclaimers that obscure the substance. Where the affected individual is a candidate in financial services or healthcare, the sensitivity of their

data means notification should ordinarily be made by telephone followed by written confirmation, not by email alone.

Exceptions to individual notification under Article 34(3) apply where: appropriate technical and organisational measures have rendered the data unintelligible (encryption); subsequent measures have ensured high risk is no longer likely; or individual notification would involve disproportionate effort, in which case a public communication is required instead. At present, Marchwood Talent has no declared encryption or pseudonymisation measures applied to AI inputs, so these exceptions are unlikely to be available. The Lead must document the reasoning for any decision not to notify individuals.

8. Vendor Escalation Route

Marchwood Talent uses AI tools operated by third-party vendors. Each vendor relationship must have a documented escalation contact held by the AI Tools Owner in an offline-accessible format. The following escalation actions apply.

For the ATS provider: the AI Tools Owner must contact the vendor's technical support and data protection contact within one hour of a Level 1 incident, stating that an incident is under investigation and requesting: immediate suspension of automated scoring for Marchwood Talent's account if technically possible; preservation of all logs, model outputs, and ranking data for the relevant period; confirmation of where candidate data is stored and processed; and a copy of the vendor's own incident response obligations under their data processing agreement. The vendor is a data processor under UK GDPR Article 28; Marchwood Talent remains the controller and bears primary regulatory responsibility.

For OpenAI (ChatGPT): Marchwood Talent must report the incident via OpenAI's enterprise privacy and security contacts and request confirmation of whether the specific data submitted can be identified, whether it was retained for model training, and whether deletion is possible. This is particularly urgent where health or criminal record data was pasted into prompts. If Marchwood Talent does not have a ChatGPT Enterprise account with appropriate data processing terms, this must be flagged to the Managing Director as an immediate structural gap.

For Microsoft 365 Copilot: escalate via the Microsoft 365 admin portal security and compliance contacts and request audit logs of Copilot interactions for the relevant period. Microsoft's data processing terms under the Microsoft Products and Services Data Protection Addendum govern this relationship and must be consulted.

For HR system and CRM AI features: contact the respective vendor's data protection officer or security team within four hours of a Level 1 incident. Request the same log preservation and data location information as above.

All vendor communications must be logged with timestamps and stored as part of the incident evidence file.

9. Post-Incident Review and the AI Incident Register

Within five business days of a Level 1 or Level 2 incident being resolved, the Data Protection Lead must convene a post-incident review meeting including the AI Tools Owner, the Managing Director, and any consultant directly involved. The review must produce a written Post-Incident Report covering: a factual account of what happened and when; which AI tool was involved and what it did; which data subjects were affected and how; the regulatory notification decision and outcome; communications sent to individuals; vendor responses; root cause assessment; and specific remediation actions with named owners and deadlines.

The Post-Incident Report must be stored in the AI Incident Register. The AI Incident Register is a permanent, access-controlled record maintained by the Data Protection Lead. Each entry must include: a unique incident reference number; the date and time the incident was identified; the severity level assigned; the AI tool or tools involved; a summary of the data and individuals affected; actions taken in the first hour; the regulatory notification decision and, if notified, the ICO reference number; the date the incident was closed; and a link to the Post-Incident Report. Level 3 incidents are logged at the time of occurrence with a shorter entry but must still be recorded.

The Register must be reviewed in full at least every six months by the Data Protection Lead and the Managing Director. Patterns across incidents — for example, repeated near-misses involving consultants pasting CVs into ChatGPT — must trigger a policy or training response, not merely individual entries. The Register is a document that the ICO may request in the event of a complaint or investigation; it must be accurate, complete, and not retrospectively amended without a dated correction note. The outcome of each post-incident review must also inform Marchwood Talent's AI tool approval process, so that lessons learned are translated into updated permissions, training, or vendor requirements.