Data Protection Policy

Grade A Recruitment

1. Purpose and Scope

Grade A Recruitment processes personal information relating to employees, candidates and work-seekers, referees, client contacts, suppliers and other individuals. This policy explains the standards Grade A applies when collecting, using, storing, sharing and disposing of personal data.

Grade A will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection and privacy legislation, as amended from time to time. This policy should be read alongside Grade A's privacy notices, Data Retention Policy, Document Protection Policy and relevant information-security and breach procedures.

2. Roles and Responsibilities

Grade A Recruitment will act as a data controller where it determines the purposes and means of processing personal data. In some circumstances Grade A may process information on behalf of another controller.

All employees are responsible for protecting personal information they access through their work and must follow Grade A's policies, procedures and security requirements. Questions, data-rights requests and data-protection concerns should be escalated promptly to the designated senior person responsible for data protection.

3. Types of Personal Data

Depending on the relationship and purpose, Grade A may process personal data including contact details, employment and work history, qualifications, references, right-to-work information, payroll and financial information, availability, assignment records and communications.

Because Grade A operates within education recruitment and safer recruitment, it may also process more sensitive information where lawful and necessary, including special category data and criminal offence information such as DBS-related information, health information, equality monitoring information and safeguarding information. Such information must receive enhanced protection and access must be limited to those with a genuine need to know.

4. Data Protection Principles

Grade A will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date where necessary;
- kept for no longer than necessary;
- processed securely using appropriate technical and organisational measures; and
- managed in a way that enables Grade A to demonstrate compliance (accountability).

5. Lawful Processing

Grade A will identify an appropriate lawful basis before processing personal data. Depending on the circumstances this may include consent, performance of a contract or steps before entering a contract, compliance with a legal obligation, vital interests, public task or legitimate interests.

Where special category data or criminal offence data is processed, Grade A will also identify any additional condition required by law and maintain appropriate safeguards and documentation. Consent will only be relied upon where it is appropriate, freely given, specific, informed and capable of being withdrawn.

6. Transparency and Privacy Information

Individuals will be provided with appropriate privacy information explaining how Grade A uses their personal data. Where information is obtained directly, the relevant privacy information will normally be provided when the information is collected. Where information is obtained from another source, Grade A will provide the required information within the applicable legal timeframe, subject to any lawful exemption.

If Grade A intends to use personal data for a materially different purpose, it will consider whether that further use is lawful and whether additional privacy information is required.

7. Data Minimisation, Accuracy and Retention

Employees should only collect, access and retain personal information that is reasonably required for a legitimate business, recruitment, employment, safeguarding or legal purpose. Records must be accurate and updated where necessary.

Personal data will be retained in accordance with Grade A's Data Retention Policy and applicable legal, regulatory, safeguarding and contractual requirements. When information is no longer required it will be securely deleted, destroyed or anonymised as appropriate.

8. Security and Confidentiality

Grade A will use appropriate technical and organisational measures to protect personal data against accidental or unlawful loss, destruction, alteration, unauthorised disclosure or access.

- Access to systems and confidential information must be restricted according to role and business need.
- Passwords, authentication details and system access must not be shared.
- Sensitive documents must not be left unattended and screens should be secured when employees are away from them.
- Personal data must only be sent to the correct authorised recipient and employees must check email addresses and attachments before sending.
- Appropriate secure methods must be used when transmitting confidential, DBS, safeguarding or other sensitive information.
- The same standards apply when working remotely or from home.
- Suspected loss, misdirection, unauthorised access or disclosure must be reported immediately.

9. Sharing Personal Data and Third Parties

Grade A may share personal data with schools and other hirers, payroll or pension providers, DBS and vetting providers, professional advisers, regulators, government bodies, software and IT providers and other service providers where there is a lawful and legitimate reason to do so.

Before sharing personal data, Grade A will consider the lawful basis, the information genuinely required, confidentiality and security. Appropriate contracts or data-processing terms will be used where required. Safeguarding information may be shared where necessary and lawful to protect children or others from harm.

10. International Transfers

Where personal data is transferred outside the UK, Grade A will ensure that an appropriate lawful transfer mechanism and safeguards are in place where required by data protection law.

11. Individual Rights

Subject to the circumstances and applicable exemptions, individuals may have rights to:

- be informed about the use of their personal data;
- access their personal data;
- have inaccurate or incomplete information corrected;
- request erasure in certain circumstances;
- request restriction of processing in certain circumstances;
- receive certain information in a portable format;
- object to certain processing, including an absolute right to object to direct marketing; and
- receive safeguards in relation to solely automated decisions that produce legal or similarly significant effects.

Requests must be passed promptly to the person responsible for data protection. Grade A will normally respond within one month, although the period may be extended where permitted by law for complex or numerous requests. Identity may be verified before information is released.

12. Automated Decision-Making and AI

Grade A will not make solely automated decisions about an individual that produce legal or similarly significant effects unless there is a lawful basis and the required safeguards are in place. Where artificial intelligence or automated tools are used to support recruitment or administration, Grade A will consider data protection, fairness, transparency, security and human oversight before use.

13. Personal Data Breaches

A personal data breach includes accidental or unlawful loss, destruction, alteration, unauthorised disclosure of or access to personal data. All actual or suspected breaches must be reported internally immediately so that Grade A can contain the incident, assess the risk and take appropriate action.

Where a breach is likely to result in a risk to individuals' rights and freedoms, Grade A will notify the Information Commissioner's Office without undue delay and, where required, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk to affected individuals, Grade A will also inform those individuals without undue delay, unless an applicable exception applies.

14. Data Protection by Design and Impact Assessments

Data protection will be considered when introducing or changing systems, processes, suppliers or technologies involving personal data. Grade A will use data minimisation, appropriate access controls and other privacy-by-design measures.

A Data Protection Impact Assessment (DPIA) will be completed where proposed processing is likely to result in a high risk to individuals' rights and freedoms, including where required for new technologies or particularly sensitive or large-scale processing.

15. Direct Marketing

Grade A will comply with applicable data protection and electronic marketing requirements when sending marketing communications. Individuals can object to direct marketing at any time and Grade A will respect and record such preferences.

16. Training, Monitoring and Accountability

Employees will receive appropriate data protection and information-security awareness. Grade A will maintain records and policies appropriate to its processing activities, review compliance, manage supplier risks and take corrective action where required.

Failure to follow this policy may result in disciplinary action and, in serious cases, may also expose individuals and Grade A to regulatory, contractual or legal consequences.

17. Concerns and Complaints

Anyone with a concern about Grade A's handling of personal information should contact Grade A so that the matter can be investigated. Individuals also have the right to raise a concern with the Information Commissioner's Office (ICO).

18. Review

This policy will be reviewed at least annually and sooner where legislation, ICO guidance, Grade A's systems or working practices materially change.

Policy owner	Operations Director / Senior Management
Updated	August 2026
Next review	August 2027 or earlier if requirements change
Related documents	Privacy Notices; Data Retention Policy; Document Protection Policy; breach and information-security procedures