

INFORMATION SECURITY AND DATA PROTECTION POLICY

Date policy issued: 08/08/2026

Date policy last reviewed: 08/08/2026

This policy will be reviewed every 12 months (as a minimum).

Review due date: 08/08/2027

Designated Safeguarding Lead contact details:

Designated Safeguarding Lead: Ethan Taberner & Joshua Heaton

Designated Safeguarding Lead Contact details: ethan.taberner@foreverteaching.co.uk / joshua.heaton@foreverteaching.co.uk / 0161 327 4385

1. Policy Statement

Forever Teaching Ltd is committed to protecting the privacy, confidentiality, integrity and availability of the personal data entrusted to us.

As an education recruitment business, Forever Teaching processes personal data relating to:

- Candidates, temporary workers, contractors and work-seekers;
- Employees, directors, consultants and prospective employees;
- Individual contacts at schools, academies, multi-academy trusts, nurseries, payroll providers, suppliers and other clients;
- Referees, emergency contacts and representatives of third-party organisations;
- Website users, prospective clients and other business contacts; and
- Individuals whose information is processed in connection with safeguarding, complaints, investigations, compliance or audit activity.

Forever Teaching will process personal data in accordance with applicable data-protection legislation, including:

- The UK General Data Protection Regulation;
- The Data Protection Act 2018;

- The Data (Use and Access) Act 2025, where applicable;
- The Privacy and Electronic Communications Regulations 2003, where applicable; and
- Any legislation, regulatory guidance or statutory code that replaces, updates or supplements these requirements.

This policy applies to all directors, employees, consultants, contractors, temporary staff, interns and any other person who processes personal data on behalf of Forever Teaching.

Failure to comply with this policy may result in disciplinary action and, in serious cases, dismissal, termination of engagement, regulatory action or legal proceedings.

2. Purpose

The purpose of this policy is to:

- Set out Forever Teaching's approach to information security and data protection;
- Ensure personal data is collected, used, shared, retained and destroyed lawfully;
- Protect the rights and freedoms of data subjects;
- Reduce the risk of accidental or unlawful loss, destruction, alteration, disclosure of or access to personal data;
- Establish clear responsibilities for employees and other authorised users;
- Support compliance with APSCo requirements, safeguarding obligations and education recruitment standards; and
- Demonstrate accountability under data-protection law.

3. Definitions

For the purpose of this policy:

Personal data means any information relating to an identified or identifiable living individual. This may include names, contact details, identification information, employment records, location information, identification numbers and online identifiers.

Processing means any operation performed on personal data, including collecting, recording, storing, organising, using, changing, retrieving, sharing, transferring, restricting, deleting or destroying it.

Data subject means the individual to whom personal data relates.

Controller means the organisation that decides why and how personal data will be processed.

Processor means an organisation that processes personal data on behalf of a controller.

Special-category data includes personal data revealing or concerning:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade-union membership;
- Genetic data;
- Biometric data used for identification;
- Health;
- Sex life; or
- Sexual orientation.

Criminal-offence data includes information relating to criminal allegations, investigations, proceedings, convictions, cautions, offences, sentencing and related security measures.

Personal data breach means a security incident that results in the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

4. Data-Protection Principles

Forever Teaching will comply with the data-protection principles. Personal data must be:

4.1 Lawful, fair and transparent

Personal data will only be processed where Forever Teaching has identified a lawful basis and has provided appropriate privacy information to the data subject.

4.2 Collected for specified purposes

Personal data will only be collected for specified, explicit and legitimate purposes. It will not be used for an incompatible purpose unless that further processing is lawful and appropriately communicated.

4.3 Adequate, relevant and limited

Forever Teaching will only collect and retain the personal data reasonably required for the relevant purpose.

4.4 Accurate and up to date

Reasonable steps will be taken to ensure personal data is accurate and, where necessary, kept up to date. Inaccurate information will be corrected or deleted without undue delay.

4.5 Retained only as long as necessary

Personal data will not be retained in an identifiable form for longer than necessary for the purpose for which it was collected, subject to legal, contractual, safeguarding, insurance and regulatory requirements.

4.6 Secure

Personal data will be protected using appropriate technical and organisational measures against unauthorised or unlawful processing and accidental loss, destruction or damage.

4.7 Accountable

Forever Teaching will maintain appropriate records and evidence to demonstrate compliance with these principles.

5. Categories of Personal Data Processed

Depending on the individual and the nature of the relationship, Forever Teaching may process:

- Name, address, telephone number and email address;
- Date of birth;
- Photographs and headshots;
- National Insurance number;
- Passport, driving licence, birth certificate and other identification information;
- Right-to-work documents and share-code results;
- Immigration status and visa information;
- Employment history, education history and reasons for employment gaps;
- Curriculum vitae, application information and interview records;
- Qualifications, registrations, professional status and training records;
- Availability, work preferences and travel information;

- Payroll, bank, tax, pension and payment information;
- Placement, assignment, booking and timesheet records;
- References and referee contact details;
- Performance, conduct, attendance and disciplinary information;
- Communications, complaints and investigation records;
- Website, device, communication and system-access information;
- Marketing preferences;
- Health, disability, fitness-to-work and reasonable-adjustment information;
- Equality-monitoring information;
- Safeguarding information;
- DBS status, barred-list results and criminal-offence information;
- Overseas police-check information;
- Childcare disqualification declarations;
- Section 128 and prohibition-check results; and
- Any other information necessary to assess suitability, meet legal obligations or manage the employment, recruitment or placement relationship.

Forever Teaching will avoid recording excessive or irrelevant information and will not retain full copies of documents where recording the verified outcome is sufficient.

6. Purposes of Processing

Forever Teaching may process personal data for the following purposes:

- Recruiting and assessing candidates and employees;
- Registering work-seekers and providing recruitment services;
- Matching candidates with suitable vacancies and assignments;
- Introducing or supplying candidates to schools, trusts, nurseries and other clients;
- Verifying identity, qualifications, employment history and suitability;
- Carrying out safeguarding and pre-employment checks;
- Obtaining and verifying references;
- Completing right-to-work checks;

- Conducting DBS, barred-list, prohibition, Section 128, overseas and childcare-disqualification checks where applicable;
- Managing temporary assignments and permanent placements;
- Managing candidate availability and communication;
- Administering payroll, timesheets, pensions, tax and invoicing;
- Monitoring performance, attendance, conduct and service quality;
- Managing employees, workers and contractors;
- Responding to complaints, safeguarding concerns, allegations and investigations;
- Complying with legal, contractual, insurance and regulatory requirements;
- Maintaining records for APSCo accreditation and other audits;
- Preventing fraud and protecting the security of our systems;
- Establishing, exercising or defending legal claims;
- Maintaining business relationships with clients and suppliers;
- Sending relevant service communications and lawful marketing;
- Carrying out business planning, reporting and quality assurance; and
- Protecting the welfare of children and adults at risk.

7. Lawful Bases for Processing

Forever Teaching will identify and document an appropriate lawful basis before processing personal data.

Depending on the circumstances, the lawful basis may include:

7.1 Performance of a contract

Processing may be necessary to:

- Take steps at an individual's request before entering into a contract;
- Register and represent candidates;
- Supply workers to clients;
- Manage assignments and placements;
- Pay temporary workers or employees; or

- Perform contractual obligations owed to candidates, workers, employees, clients or suppliers.

7.2 Legal obligation

Processing may be necessary to comply with obligations relating to:

- Right-to-work checks;
- Employment law;
- Tax, payroll and pension administration;
- Safeguarding;
- Recruitment and supply of workers;
- Health and safety;
- Equality law;
- Regulatory investigations;
- Court orders; or
- Other statutory requirements.

7.3 Legitimate interests

Forever Teaching may process personal data where it is necessary for legitimate business interests and those interests are not overridden by the rights and freedoms of the data subject.

Legitimate interests may include:

- Providing recruitment services;
- Maintaining relationships with candidates and clients;
- Finding suitable work for registered candidates;
- Introducing candidates to relevant clients;
- Verifying information supplied during registration;
- Preventing fraud;
- Maintaining network and information security;
- Managing complaints and disputes;
- Recovering debts;
- Protecting Forever Teaching's legal position; and

- Communicating with existing or prospective business contacts.

Where legitimate interests are relied upon, Forever Teaching will consider necessity, proportionality and the reasonable expectations of the individual. A Legitimate Interests Assessment will be completed where appropriate.

7.4 Consent

Consent may be used where the individual has been given a genuine choice and can withdraw consent without detriment.

Consent will not normally be relied upon where another lawful basis is more appropriate, particularly where there is an imbalance of power or where the processing is necessary to provide recruitment or employment services.

Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

7.5 Vital interests

In exceptional circumstances, Forever Teaching may process personal data where necessary to protect someone's life.

7.6 Public task

Forever Teaching will only rely on public-task grounds where it is legally entitled to do so.

8. Special-Category and Criminal-Offence Data

Special-category and criminal-offence data will only be processed where:

- An Article 6 lawful basis applies; and
- A separate condition under Article 9 of the UK GDPR or Schedule 1 of the Data Protection Act 2018 applies, as appropriate.

Relevant conditions may include:

- Employment, social-security and social-protection obligations;
- Preventive or occupational medicine and assessment of working capacity;
- Establishing, exercising or defending legal claims;
- Explicit consent, where genuinely appropriate;
- Safeguarding children and individuals at risk;
- Preventing or detecting unlawful acts;
- Protecting the public against dishonesty or malpractice;

- Equality-of-opportunity monitoring; and
- Other substantial-public-interest conditions permitted by law.

Where legally required, Forever Teaching will maintain an Appropriate Policy Document explaining:

- The Schedule 1 conditions relied upon;
- How the data-protection principles are applied;
- Retention and deletion arrangements; and
- The safeguards applied to sensitive information.

8.1 DBS and criminal-offence information

Forever Teaching will treat DBS and criminal-offence information as strictly confidential.

Access will be restricted to authorised compliance personnel, directors and Designated Safeguarding Leads where necessary.

Forever Teaching will:

- Only request criminal-record information where lawful and relevant;
- Ensure candidates are informed about the nature of the check;
- Apply the Rehabilitation of Offenders Act 1974 and relevant Exceptions Orders;
- Avoid retaining copies of DBS certificates for longer than permitted or necessary;
- Record the result, certificate details and check date where appropriate;
- Complete a documented risk assessment where information is disclosed;
- Avoid sharing the detailed content of a disclosure unless lawful, necessary and proportionate; and
- Store disclosure forms and risk assessments separately or with enhanced access restrictions.

A candidate will not automatically be rejected because information appears on a DBS certificate. Any disclosure will be considered fairly in accordance with Forever Teaching's Rehabilitation of Offenders SOP and Criminal Disclosure Risk Assessment process.

9. Transparency and Privacy Information

Forever Teaching will provide appropriate privacy information to individuals when personal data is collected, or within the period required by law where information is obtained from another source.

Privacy information will explain, as applicable:

- Forever Teaching's identity and contact details;
- The purposes of processing;
- The lawful bases relied upon;
- The categories of data processed;
- Where the information came from;
- Who the information may be shared with;
- How long the information will be retained;
- Whether data may be transferred internationally;
- The individual's rights;
- The right to complain to the Information Commissioner's Office;
- Whether providing the information is legally or contractually required;
- The consequences of not providing relevant information; and
- Any automated decision-making or profiling.

Privacy notices must be written clearly and must remain accessible to the relevant individuals.

10. Collection and Verification of Candidate Information

Candidate information may be collected through:

- Application forms;
- Curriculum vitae;
- Registration forms;
- Interviews;
- Telephone and email communications;
- Job boards and professional networking platforms;
- Publicly available professional information;
- Referees;
- Clients;
- Government and regulatory checking services;

- DBS and identity-check providers;
- Payroll providers;
- Former employers and education providers; and
- Other recruitment or compliance partners.

Forever Teaching will take reasonable steps to verify information relevant to a candidate's identity, qualifications, experience, employment history, right to work, safeguarding status and suitability.

Where online searches are undertaken as part of safer recruitment:

- Candidates will be informed that searches may take place;
- Searches will be relevant, proportionate and limited to information that may affect suitability;
- Protected characteristics and irrelevant personal information will not be used to make recruitment decisions;
- Any relevant concern will normally be raised with the candidate before a decision is made; and
- The date, purpose and outcome of the search will be documented appropriately.

11. Sharing Personal Data

Personal data will only be shared where there is a lawful basis, a legitimate and defined purpose, and the disclosure is necessary and proportionate.

Forever Teaching may share personal data with:

- Schools, academies, multi-academy trusts, nurseries and other clients;
- Prospective employers;
- Payroll and umbrella companies selected or approved by the worker;
- Pension, tax and accounting providers;
- DBS, identity and right-to-work checking providers;
- Training providers;
- Insurers, auditors and professional advisers;
- IT, CRM, communication and cloud-storage providers;
- Government departments, regulators, safeguarding partners and law-enforcement bodies;

- Courts and legal representatives;
- APSCo and other accreditation or audit bodies; and
- Other organisations where disclosure is legally required or necessary to protect children or adults at risk.

Forever Teaching will not routinely send a candidate's CV or profile to a client without an appropriate lawful basis and without making candidates aware that their information may be used in this way.

Only information relevant to the proposed role or safeguarding requirements will be supplied to a client.

Safeguarding information may be shared without consent where necessary to protect a child or adult at risk, comply with a legal obligation or support a lawful safeguarding investigation. Information will be shared on a need-to-know basis.

12. Data Processors and Third-Party Suppliers

Before appointing a processor, Forever Teaching will take reasonable steps to ensure the supplier provides sufficient guarantees that personal data will be protected.

A written data-processing agreement must be in place where required. The agreement must address:

- The subject matter and duration of processing;
- The nature and purpose of processing;
- The types of personal data and categories of data subject;
- Confidentiality;
- Security obligations;
- Use of subprocessors;
- Assistance with data-subject rights;
- Assistance with breach management;
- Return or deletion of data at the end of the arrangement; and
- Audit and compliance requirements.

Third-party access to systems and information must be limited to what is necessary.

13. International Transfers

Personal data will not be transferred outside the United Kingdom unless the transfer is lawful and appropriate safeguards are in place.

Safeguards may include:

- UK adequacy regulations;
- The UK International Data Transfer Agreement;
- The UK Addendum to approved standard contractual clauses;
- Legally permitted exceptions; or
- Another approved transfer mechanism.

Where required, Forever Teaching will complete a transfer-risk assessment and implement supplementary security measures.

14. Information Security

Forever Teaching will use appropriate technical and organisational measures based on the nature of the information, the risks presented by processing and the potential impact on individuals.

Measures may include:

- Unique user accounts;
- Strong passwords;
- Multi-factor authentication where available;
- Role-based access controls;
- Secure CRM and cloud-storage systems;
- Encryption in transit and, where appropriate, at rest;
- Antivirus, firewall and endpoint protection;
- Supported and regularly updated software;
- Secure backups;
- Device locking;
- Controlled downloading and printing;
- Secure disposal;
- Confidentiality obligations;
- Staff training;
- Regular access reviews;
- Incident-reporting procedures; and

- Business-continuity and recovery arrangements.

Employees must not attempt to bypass or disable security controls.

15. Employee Responsibilities

Anyone processing personal data on behalf of Forever Teaching must:

- Only access information required for their role;
- Only use personal data for authorised business purposes;
- Follow this policy and all related procedures;
- Keep passwords and authentication details confidential;
- Lock their screen whenever leaving a device unattended;
- Use approved systems, devices and communication channels;
- Check recipients carefully before sending emails or attachments;
- Use secure transfer methods when sending sensitive information;
- Avoid including unnecessary personal data in email subject lines;
- Use blind carbon copy where appropriate when emailing multiple unrelated recipients;
- Keep desks, screens and paperwork secure;
- Avoid discussing confidential information where unauthorised people may overhear;
- Ensure records are accurate, professional and relevant;
- Report inaccuracies when identified;
- Report suspicious emails, malware or unauthorised access immediately;
- Report actual or suspected data breaches immediately;
- Securely dispose of information in accordance with the retention schedule; and
- Complete mandatory data-protection and information-security training.

Employees must not:

- Share accounts or passwords;
- Access candidate or client records out of curiosity;
- Send personal data to personal email accounts;
- Save personal data to unauthorised storage services;

- Use unapproved messaging applications for sensitive information;
- Download personal data to personal devices without authorisation;
- Photograph personal data using a personal device;
- Leave personal data unattended in vehicles or public places;
- Remove paper files from the office without a legitimate reason and appropriate authorisation; or
- Disclose personal data to an unauthorised person.

16. Email and Communication Security

Before sending personal data, employees must:

- Confirm the recipient's identity and email address;
- Ensure the recipient is authorised to receive the information;
- Attach the correct document;
- Limit the information to what is necessary;
- Password-protect or encrypt sensitive documents where appropriate;
- Send passwords through a separate channel;
- Avoid sending multiple candidate records in one attachment unless necessary;
- Consider whether secure CRM access or another controlled method would be safer; and
- Remove unnecessary previous correspondence from email chains.

Any email sent to the wrong recipient must be reported immediately as a suspected personal data breach.

17. Remote Working and Mobile Devices

When working remotely, staff must:

- Use only authorised devices and systems;
- Keep devices physically secure;
- Prevent family members or other unauthorised people from using work devices;
- Avoid working with sensitive information where screens or conversations can be observed;
- Use secure internet connections;

- Avoid accessing sensitive systems through unsecured public Wi-Fi unless an approved secure connection is used;
- Lock screens when unattended;
- Store paper records securely;
- Return or securely destroy documents when no longer needed; and
- Immediately report lost or stolen devices.

Personal data must not be permanently stored on local device drives unless authorised and appropriately protected.

18. Physical Records and Clear-Desk Requirements

Paper records containing personal data must:

- Be kept to a minimum;
- Be stored in locked cupboards or controlled-access areas;
- Not be left unattended on desks, printers or in meeting rooms;
- Not be taken off-site without authorisation;
- Be returned promptly to secure storage;
- Be disposed of through confidential-waste or cross-cut shredding; and
- Be recorded when removed from their normal storage location where appropriate.

At the end of each working day, personal and confidential information must be secured.

19. Accuracy and Record Keeping

Employees must ensure that information entered into the CRM or other business system is:

- Accurate;
- Factual;
- Relevant;
- Necessary;
- Respectful and professional;
- Clearly dated; and
- Attributable to the person making the entry.

Opinions must be clearly identified as opinions and supported by relevant facts.

Personal notes must not be used as an alternative to updating the authorised business record.

Candidates, workers and employees should be encouraged to notify Forever Teaching when their information changes.

20. Data Retention and Secure Destruction

Forever Teaching will maintain a documented retention schedule covering candidate, worker, employee, client, compliance, financial, safeguarding and marketing records.

Retention periods will be based on:

- The purpose for which the information was collected;
- Statutory retention requirements;
- Employment and recruitment obligations;
- Limitation periods for legal claims;
- Safeguarding considerations;
- Insurance requirements;
- Contractual requirements;
- APSCo or regulatory requirements; and
- Whether the individual remains actively registered or engaged.

Information that is no longer required will be:

- Securely deleted;
- Anonymised; or
- Securely destroyed.

Deletion must include copies held in email accounts, shared folders, local downloads and paper files where reasonably practicable.

Information subject to a complaint, legal claim, investigation, safeguarding concern, regulatory request or litigation hold must not be destroyed until authorised.

21. Individual Rights

Subject to legal conditions and exemptions, individuals may have the right to:

- Be informed about processing;

- Access their personal data;
- Request correction of inaccurate data;
- Request deletion of personal data;
- Request restriction of processing;
- Object to processing;
- Receive certain information in a portable format;
- Withdraw consent;
- Object to direct marketing;
- Receive information about automated decision-making; and
- Complain to the Information Commissioner's Office.

All staff must recognise that an individual does not need to use the words “subject access request” for a request to be valid.

Any request concerning an individual's data-protection rights must be forwarded immediately to the designated data protection contacts.

Employees must not attempt to respond to such requests without authorisation.

22. Subject Access Requests

A subject access request may be made verbally or in writing and to any member of staff.

On receipt, the request must be sent immediately to:

Designated data protection contacts: Ethan Taberner and Joshua Heaton

Email: ethan.taberner@foreverteaching.co.uk and joshua.heaton@foreverteaching.co.uk

Forever Teaching will:

- Record the date the request was received;
- Confirm the identity of the requester where reasonably necessary;
- Clarify the scope where appropriate;
- Search relevant systems and records;
- Protect the rights of third parties;
- Apply any lawful exemptions carefully;
- Provide the response securely; and

- Respond within the legally required period.

The usual response period is one month. The deadline may be extended where legally permitted, but the individual must be informed within the initial response period.

Requests will normally be handled free of charge. A reasonable fee may only be charged where permitted by law.

23. References and Third-Party Information

Requests for access to references or other third-party information must be referred to the designated data protection contacts.

Forever Teaching will consider:

- Whether the information is the requester's personal data;
- Whether the reference was received or provided by Forever Teaching;
- Any applicable legal exemption;
- The rights and confidentiality of the referee;
- Whether the third party has consented to disclosure;
- Whether it is reasonable to disclose without consent; and
- Whether information can be redacted.

References will not automatically be withheld or disclosed. Each request will be considered individually and documented.

24. Direct Marketing

Marketing communications will only be sent where lawful.

Forever Teaching will:

- Respect opt-out requests;
- Maintain suppression records where necessary;
- Clearly identify the sender;
- Provide a simple way to unsubscribe;
- Avoid sending unsolicited electronic marketing where consent is required and has not been obtained; and
- Distinguish recruitment-service communications from direct marketing.

An individual who objects to direct marketing will be removed from active marketing lists promptly. A minimal suppression record may be retained to ensure the individual is not contacted again.

25. Data Protection by Design and Default

Data protection must be considered when introducing or changing:

- IT systems;
- CRM functionality;
- Recruitment processes;
- Candidate-screening tools;
- Artificial-intelligence tools;
- Monitoring arrangements;
- Marketing systems;
- Suppliers;
- Data-sharing arrangements; or
- Any process involving significant personal data.

Forever Teaching will ensure that, by default:

- Only necessary information is collected;
- Access is restricted;
- Retention is limited;
- Privacy settings are appropriately configured; and
- Data-protection risks are addressed before processing begins.

26. Data Protection Impact Assessments

A Data Protection Impact Assessment must be considered where processing is likely to result in a high risk to individuals.

Examples may include:

- Large-scale processing of special-category or criminal-offence data;
- Systematic monitoring;
- New screening or profiling technology;
- Artificial-intelligence-supported recruitment decisions;

- Biometric identification;
- Combining data from multiple sources;
- Significant automated decision-making; or
- Processing involving vulnerable individuals.

A high-risk processing activity must not begin until the assessment has been reviewed and approved.

Where residual high risk remains, Forever Teaching will consider whether consultation with the Information Commissioner's Office is required.

27. Automated Decision-Making and Artificial Intelligence

Forever Teaching will not make a decision producing legal or similarly significant effects about a candidate or employee solely through automated processing unless this is lawful and appropriate safeguards are in place.

Where artificial-intelligence or automated tools are used:

- Human oversight must be maintained;
- Outputs must be checked for accuracy;
- Bias and discrimination risks must be assessed;
- Confidential information must not be entered into unauthorised public tools;
- Candidates must be given appropriate privacy information;
- Decisions must not be based solely on unverified automated outputs; and
- Use of the tool must be approved by a Director.

28. Personal Data Breaches

All actual or suspected personal data breaches must be reported immediately to the designated data protection contacts.

Examples include:

- An email sent to the wrong recipient;
- A lost laptop or telephone;
- A misplaced candidate file;
- Unauthorised access to the CRM;
- A compromised password;

- Malware or ransomware;
- Accidental deletion or alteration;
- Inappropriate disclosure to a client;
- Posting personal data to the wrong address;
- Loss of an unencrypted storage device; or
- Unauthorised access by an employee.

Employees must:

- Report the incident immediately;
- Take reasonable steps to contain the incident;
- Preserve relevant evidence;
- Avoid concealing or independently investigating the matter;
- Avoid contacting affected individuals unless instructed; and
- Cooperate with the investigation.

Forever Teaching will document:

- What happened;
- The categories and approximate number of individuals affected;
- The type and volume of information involved;
- The likely consequences;
- Containment and recovery measures;
- The assessment of risk;
- Whether the ICO was notified;
- Whether affected individuals were informed; and
- Lessons and corrective action.

Where a breach is likely to result in a risk to individuals' rights and freedoms, Forever Teaching will notify the ICO 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, affected individuals will also be informed without undue delay unless an exemption applies.

29. Safeguarding and Information Sharing

Nothing in this policy prevents appropriate information sharing for safeguarding purposes.

Where there is a concern about the safety or welfare of a child or adult at risk, employees must:

- Follow Forever Teaching's Safeguarding Policy;
- Refer the matter to the Designated Safeguarding Lead;
- Record the concern accurately;
- Share only information that is necessary and relevant;
- Share information securely;
- Document the decision and reasons for sharing or not sharing; and
- Avoid promising absolute confidentiality.

Consent is not always required to share information for safeguarding purposes. Where seeking consent would place someone at risk, prejudice an investigation or cause an unreasonable delay, information may be shared where there is another lawful basis.

30. Training and Awareness

All employees and other relevant personnel will receive data-protection and information-security training:

- As part of induction;
- At least annually;
- When policies or systems materially change; and
- Following an incident or identified knowledge gap.

Training completion will be recorded.

Employees with specialist responsibilities may receive additional training concerning:

- Subject access requests;
- DBS and criminal-offence information;
- Data breaches;
- Safeguarding;
- Data Protection Impact Assessments; and
- Supplier and processor management.

31. Monitoring and Audit

Forever Teaching may monitor compliance through:

- File audits;
- CRM audits;
- Access reviews;
- Training records;
- Security testing;
- Breach and incident reviews;
- Supplier reviews;
- Retention exercises;
- APSCo audits; and
- Internal quality-assurance checks.

Monitoring will itself be conducted lawfully, transparently and proportionately.

Any non-compliance will be recorded, investigated and addressed.

32. Complaints

Any concern about Forever Teaching's handling of personal data should be sent to:

Ethan Taberner and Joshua Heaton

Forever Teaching Ltd

Email: ethan.taberner@foreverteaching.co.uk and
joshua.heaton@foreverteaching.co.uk

Forever Teaching will investigate complaints fairly and respond within a reasonable period.

Individuals also have the right to complain to the Information Commissioner's Office.

33. Roles and Responsibilities

Directors

The Directors are responsible for:

- Overall compliance;
- Approving this policy;
- Providing appropriate resources;

- Managing serious incidents;
- Ensuring risks are appropriately assessed; and
- Promoting a culture of confidentiality and accountability.

Designated data protection contacts

The designated contacts are responsible for:

- Providing guidance;
- Coordinating rights requests;
- Managing breach assessments;
- Maintaining relevant records;
- Supporting policy reviews;
- Monitoring compliance; and
- Liaising with the ICO where required.

Compliance personnel

Compliance personnel are responsible for:

- Applying enhanced safeguards to candidate compliance information;
- Restricting access to sensitive records;
- Completing and recording checks accurately;
- Following retention requirements;
- Escalating disclosures and safeguarding concerns; and
- Maintaining evidence for audit.

Employees and authorised users

All employees and authorised users are personally responsible for:

- Following this policy;
- Protecting information;
- Completing training;
- Reporting incidents; and
- Seeking advice where uncertain.

34. Related Policies and Documents

This policy should be read alongside:

- Candidate Privacy Notice;
- Employee Privacy Notice;
- Client Privacy Notice, where applicable;
- Data Retention Schedule;
- Appropriate Policy Document;
- Personal Data Breach Procedure;
- Subject Access Request Procedure;
- Safeguarding Policy;
- Safer Recruitment Policy;
- Rehabilitation of Offenders SOP;
- Criminal Disclosure Form;
- Criminal Disclosure Risk Assessment;
- DBS Policy;
- Overseas Checks Procedure;
- Complaints Policy;
- Whistleblowing Policy;
- Business Continuity Plan;
- Acceptable Use or IT Security Policy;
- Record of Processing Activities;
- Legitimate Interests Assessments; and
- Processor and data-sharing agreements.

35. Policy Review

This policy will be reviewed:

- At least annually;
- Following a personal data breach;
- Following a significant complaint;
- Following an audit finding;

- When relevant legislation or regulatory guidance changes;
- When Forever Teaching adopts a significant new system or process; or
- When Forever Teaching's services or processing activities materially change.

All amendments must be approved by the Directors and communicated to relevant employees.

36. Approval

Approved by: Ethan Taberner and Joshua Heaton

Position: Directors

Approval date: 22 July 2026