



Data Protection and GDPR Policy

REVIEWED: August 2026

NEXT REVIEW DATE: August 2027

REVIEWED BY: Mark Davis, Data Protection Officer

1. INTRODUCTION

Smile Education Limited ("Smile", "we", "us" or "our") holds and processes personal data about employees, workers, job applicants, candidates, clients, suppliers and other individuals for a variety of legitimate business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing the collection, use, storage, sharing and other processing of personal data to which they have access in the course of their work.

All personal data must be processed in accordance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), as amended, and other applicable data protection and privacy legislation ("Data Protection Laws").

Staff must consult the Data Protection Officer ("DPO") before any significant new data processing activity is initiated where appropriate, so that relevant data protection requirements can be considered from the outset.

2. DEFINITIONS

Business purposes

The purposes for which personal data may be used by us include personnel, administrative, financial, regulatory, payroll, recruitment and business development purposes.

Business purposes include:

- compliance with our legal, regulatory and corporate governance obligations and good practice;
- gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests;
- ensuring business policies are adhered to, including policies covering email and internet use;
- operational purposes, including recording transactions, training and quality control, maintaining confidentiality and security, vetting and checking;
- investigating complaints;
- checking references and qualifications;
- safeguarding and safer recruitment;
- monitoring and managing staff access to systems and facilities;



- managing staff absence, administration and assessments;
- monitoring staff conduct and disciplinary matters;
- marketing our business where permitted by applicable law; and
- improving our services.

Personal Data

Personal Data means any information relating to an identified or identifiable living individual.

This may include information relating to job applicants, candidates, current and former employees, agency workers, contractors and other staff, clients, suppliers and marketing contacts.

Personal Data we gather may include contact details, educational background, financial and pay information, certificates and qualifications, education and skills, employment history, nationality, job title and CV information.

Special Category Personal Data

Special Category Personal Data includes Personal Data revealing or concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data where used for the purpose of uniquely identifying an individual;
- health;
- sex life; or
- sexual orientation.

Special Category Personal Data is subject to additional protections under Data Protection Laws and must only be processed where an appropriate lawful basis and additional condition for processing apply.

Criminal Offence Data

Criminal Offence Data includes Personal Data relating to criminal convictions and offences, allegations of criminal activity, related proceedings and related security measures.

This includes information obtained through criminal record and DBS checks.

Criminal Offence Data is subject to additional legal requirements and must only be processed where permitted by Data Protection Laws.

3. SCOPE

This policy applies to all staff. All staff must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to data protection, information security, internet and email use and data retention.



We may supplement or amend this policy by issuing additional policies and guidelines from time to time. Any new or materially modified policy will be communicated to relevant staff.

Who is responsible for this policy?

Mark Davis is Smile Education Limited's Data Protection Officer and has overall responsibility for the day-to-day implementation and monitoring of this policy.

All references in this policy to the "DPO" or "Data Protection Officer" mean Mark Davis or any formally appointed successor to that role.

4. OUR PROCEDURES

Fair and lawful processing

We must process Personal Data lawfully, fairly and transparently and in accordance with individuals' rights.

Before processing Personal Data, Smile must identify and document an appropriate lawful basis under Data Protection Laws.

Depending on the circumstances, the lawful basis may include:

- consent;
- performance of a contract or taking steps at an individual's request before entering into a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task in the public interest, where applicable;
- recognised legitimate interests, where applicable under Data Protection Laws; or
- Smile's legitimate interests or those of a third party, provided those interests are not overridden by the rights and interests of the individual.

Consent is not required for all processing and must not be treated as the default lawful basis.

For example, recruitment, payroll, employment administration, safeguarding, compliance checks and other legal or regulatory activities may be processed under another appropriate lawful basis.

Where Smile relies upon consent, the consent must satisfy the requirements of Data Protection Laws, including being freely given, specific, informed and capable of being withdrawn.

Where Special Category Personal Data or Criminal Offence Data is processed, Smile must also identify and document any additional condition or legal authority required under Data Protection Laws.

The Data Protection Officer's responsibilities

The DPO's responsibilities include:

- keeping the board updated about data protection responsibilities, risks and issues;
- reviewing data protection procedures and policies regularly;
- arranging appropriate data protection training and advice for staff;



- answering data protection questions from staff, board members and other stakeholders;
- overseeing responses to individuals exercising their data protection rights;
- advising on Data Protection Impact Assessments where required;
- overseeing Personal Data breach management;
- advising on international transfers of Personal Data; and
- reviewing data protection provisions in arrangements with third parties that process Personal Data.

Responsibilities of the IT Department

The IT Department is responsible for:

- ensuring systems, services, software and equipment meet appropriate security standards;
- checking and scanning security hardware and software regularly;
- maintaining appropriate technical safeguards;
- supporting secure access controls and backups; and
- assessing third-party services, including cloud services, which Smile is considering using to store or process Personal Data.

Responsibilities of the Marketing Manager

The Marketing Manager is responsible for:

- approving appropriate data protection and privacy statements used in marketing communications;
- addressing data protection queries relating to marketing activity; and
- coordinating with the DPO to ensure marketing initiatives comply with applicable data protection and electronic marketing laws and this policy.

Lawful basis and purpose

All processing must be carried out for a specified and legitimate purpose and must have an appropriate lawful basis.

Smile will identify and document the lawful basis applicable to relevant processing activities and communicate the required information to individuals through appropriate privacy notices.

5. SPECIAL CATEGORY PERSONAL DATA AND CRIMINAL OFFENCE DATA

Special Category Personal Data requires additional protection because of its sensitive nature.

Smile will only process Special Category Personal Data where:

1. an appropriate lawful basis for processing Personal Data applies; and
2. an appropriate additional condition for processing Special Category Personal Data applies under Data Protection Laws.

Explicit consent may be appropriate in some circumstances but is not the only condition available and should not automatically be relied upon.

Criminal Offence Data is subject to separate requirements. Smile will only process Criminal Offence Data where there is an appropriate lawful basis and the processing is authorised by applicable law.



Criminal record and DBS checks must only be carried out where legally permitted and appropriate to the role or purpose concerned. Such processing must not be based solely upon an individual's consent where another legal condition is required.

Where required by the DPA 2018, Smile will maintain an appropriate policy document covering the processing of Special Category Personal Data and/or Criminal Offence Data.

6. ACCURACY, RELEVANCE AND DATA MINIMISATION

We will take reasonable steps to ensure that Personal Data we process is accurate and, where necessary, kept up to date.

Personal Data must be adequate, relevant and limited to what is necessary for the purpose for which it is processed.

We will not use Personal Data for a new and incompatible purpose unless permitted under Data Protection Laws.

Individuals may ask us to correct inaccurate Personal Data relating to them.

If you believe information held by Smile is inaccurate, you should record that its accuracy is disputed where appropriate and inform the DPO, Mark Davis.

7. YOUR PERSONAL DATA

Staff must take reasonable steps to ensure that Personal Data Smile holds about them is accurate and up to date.

If your personal circumstances change in a way that affects information held by Smile, please notify the appropriate internal contact or the DPO so that the relevant records can be updated.

8. DATA SECURITY

Personal Data must be kept secure against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Where another organisation processes Personal Data on Smile's behalf, Smile will ensure that appropriate contractual, organisational and security arrangements are in place as required by Data Protection Laws.

Staff must comply with Smile's information security procedures at all times.

9. STORING DATA SECURELY

The following requirements apply to the storage of Personal Data:

- printed Personal Data must be stored securely where unauthorised personnel cannot access it;
- confidential printed documents must be securely destroyed when they are no longer required;
- Personal Data stored electronically must be protected using appropriate access controls and security measures;
- staff must use strong passwords and comply with Smile's password and access-control requirements;



- removable media containing Personal Data must be appropriately protected and securely stored;
- cloud services used to store or process Personal Data must be approved through Smile's appropriate internal process, involving the DPO and/or IT as required;
- servers and systems containing Personal Data must be appropriately secured;
- Personal Data must be backed up in accordance with Smile's backup procedures;
- Personal Data stored or accessed on laptops, tablets or smartphones must be appropriately secured and only used for authorised business purposes; and
- systems containing Special Category Personal Data or Criminal Offence Data must have security measures appropriate to the increased risks associated with that information.

10. DATA RETENTION

Personal Data must not be kept for longer than is necessary for the purpose for which it was collected or as required by law.

Appropriate retention periods will be determined by taking account of:

- the purpose for which the information was collected;
- legal and regulatory requirements;
- contractual requirements;
- safeguarding obligations;
- the establishment, exercise or defence of legal claims; and
- Smile's applicable data retention policies and schedules.

At the end of the applicable retention period, Personal Data must be securely deleted, destroyed or anonymised unless there is a lawful reason to retain it for longer.

11. INTERNATIONAL DATA TRANSFERS

Personal Data must not be transferred outside the UK without Smile's prior approval and compliance with applicable Data Protection Laws.

Staff must consult the DPO before arranging or commencing a transfer of Personal Data outside the UK unless the transfer has already been approved under an established Smile process.

Where an international transfer is a restricted transfer under the UK GDPR, Smile will ensure that an appropriate lawful transfer mechanism is in place. Depending on the circumstances, this may include:

- applicable UK adequacy regulations;
- appropriate safeguards recognised under UK Data Protection Laws, including an approved International Data Transfer Agreement or UK Addendum where appropriate; or
- a permitted statutory exception.

Any required transfer risk assessment or other assessment must also be completed before the transfer takes place.

Consent will not automatically be required for an international transfer. The appropriate transfer mechanism must be determined in accordance with Data Protection Laws.



12. INDIVIDUAL RIGHTS AND SUBJECT ACCESS REQUESTS

Under the UK GDPR and Data Protection Act 2018, individuals have rights in relation to their Personal Data, subject to applicable conditions and exemptions.

These may include the right to:

- be informed about how their Personal Data is processed;
- request access to their Personal Data;
- request correction of inaccurate Personal Data;
- request erasure of Personal Data in certain circumstances;
- request restriction of processing;
- object to certain processing;
- receive certain Personal Data in a portable format;
- withdraw consent where processing is based on consent; and
- exercise rights relating to certain automated decision-making, where applicable.

If you receive a subject access request or another request relating to an individual's data protection rights, you must refer it promptly to the DPO.

Staff must not ignore, delay or attempt to deal informally with such a request without following Smile's relevant procedure.

Individuals wishing to exercise their rights in relation to information held by Smile should contact the DPO.

13. DIRECT MARKETING

Individuals have the right to object to the processing of their Personal Data for direct marketing purposes.

If an individual objects to direct marketing or unsubscribes from marketing communications, that request must be acted upon promptly and appropriately recorded.

Staff must comply with applicable Data Protection Laws and electronic marketing rules when carrying out direct marketing.

Before starting a new form of direct marketing activity, staff should consult the DPO where advice is required.

14. TRAINING

All relevant staff will receive appropriate training on this policy and their data protection responsibilities.

New joiners will receive data protection training as part of the induction process.

Refresher or additional training will be provided periodically and where appropriate following substantial changes in legislation, guidance, Smile's processing activities or this policy.

Completion of required data protection training is compulsory.



15. PRIVACY NOTICE AND TRANSPARENCY

Smile is committed to being transparent about how it collects and uses Personal Data.

Individuals will be provided with appropriate privacy information explaining, as required by Data Protection Laws:

- what Personal Data is collected;
- the purposes for which it is used;
- the applicable lawful basis or bases;
- where the information was obtained where relevant;
- who it may be shared with;
- how long it will be retained or how retention periods are determined;
- whether international transfers take place;
- the individual's data protection rights; and
- how to raise a concern or complaint.

What information may be collected?

Depending on the individual's relationship with Smile, information may include:

- CVs;
- names and contact information;
- addresses;
- dates of birth;
- employment history;
- qualifications and certificates;
- identity and right-to-work information;
- National Insurance information;
- financial and payroll information; and
- safeguarding information and documentation, including DBS information where appropriate and legally permitted.

Further information about retention is contained in Smile's data retention policy.

Who collects Personal Data?

Personal Data may be collected by authorised Smile Education staff, including Recruitment Consultants, Administrators, Managers and Directors.

How is Personal Data collected?

Smile may obtain Personal Data from sources including:

- our website;
- social media and professional networking platforms;
- telephone and email enquiries;
- job applications;
- CV databases and recruitment platforms;



- individuals directly;
- clients and other organisations;
- referees; and
- other lawful sources relevant to recruitment and employment activities.

Why is Personal Data collected and how will it be used?

Smile processes Personal Data for purposes connected with its recruitment and employment services and other legitimate business activities.

Depending on the circumstances, this may include:

- finding and arranging work for candidates;
- assessing suitability for roles;
- communicating employment opportunities;
- verifying qualifications, identity and eligibility to work;
- safeguarding and compliance checks;
- administering placements;
- managing payroll and payments;
- complying with legal and regulatory requirements;
- maintaining business records;
- providing professional development opportunities; and
- communicating relevant service or business information.

Each processing activity must be supported by an appropriate lawful basis.

Who will Personal Data be shared with?

Where necessary and lawful, Personal Data may be shared with third parties such as:

- prospective or existing clients;
- payroll providers;
- background checking and safeguarding providers;
- professional advisers;
- regulators and public authorities;
- IT and technology providers; and
- other service providers acting on Smile's behalf.

Information must only be shared where there is an appropriate lawful basis and where applicable contractual, confidentiality and security safeguards are in place.

Where consent is the appropriate lawful basis, Personal Data will only be processed or shared within the scope of the consent given. Where another lawful basis applies, Smile does not need to obtain consent solely because Personal Data is being processed or shared.

16. CONDITIONS AND LAWFUL BASES FOR PROCESSING

Smile will ensure that every processing activity has an identified and documented lawful basis.



Staff responsible for processing Personal Data must understand the purpose of the processing and ensure that the relevant requirements are followed.

Smile's privacy information will explain the lawful basis or bases relied upon where required.

Consent

Consent is one possible lawful basis for processing Personal Data. It is not required for every processing activity.

Where Smile relies upon consent, the consent must be valid under Data Protection Laws and individuals must be able to withdraw it as easily as they gave it.

Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn. Smile may also continue to process relevant information after consent is withdrawn where another lawful basis applies to that processing or retention.

Criminal record checks

Criminal record and DBS checks must only be undertaken where appropriate and legally permitted.

Smile will identify and document the lawful basis and any additional legal condition required for processing Criminal Offence Data.

Criminal record checks will not be undertaken solely on the basis of an individual's consent where applicable law requires additional authority.

17. DATA PORTABILITY

Where the right to data portability applies, an individual may request to receive relevant Personal Data in a structured, commonly used and machine-readable format and may have the right to request that it is transmitted to another controller where technically feasible.

Requests will be handled in accordance with the requirements and timescales under Data Protection Laws.

18. RIGHT TO ERASURE

An individual may request the deletion or removal of Personal Data in circumstances where the right to erasure applies.

The right to erasure is not absolute. Smile may retain Personal Data where continued processing is permitted or required by law, including where necessary to comply with a legal obligation or for the establishment, exercise or defence of legal claims.

Where appropriate, Smile will also communicate an erasure request to relevant recipients of the Personal Data as required by Data Protection Laws.



19. DATA PROTECTION BY DESIGN AND DEFAULT

Smile will take data protection requirements into account when developing new projects, systems, processes and services involving Personal Data.

Appropriate technical and organisational measures should be considered from the outset and throughout the lifecycle of the processing.

Where processing is likely to result in a high risk to the rights and freedoms of individuals, Smile will carry out a Data Protection Impact Assessment (“DPIA”) before commencing the relevant processing.

The DPO will provide advice on DPIAs and monitor their completion where required.

Appropriate privacy settings and data-minimisation measures should be applied by default where relevant.

20. DATA AUDIT AND RECORDS

Smile will maintain appropriate records of its Personal Data processing activities.

Regular reviews and audits may be undertaken to identify and manage data protection risks.

Relevant records should identify, where appropriate:

- what Personal Data is held;
- why it is processed;
- the lawful basis for processing;
- where it is stored;
- who it is shared with;
- who is responsible for it;
- applicable retention periods;
- international transfers; and
- relevant security or compliance measures.

21. REPORTING PERSONAL DATA BREACHES

All staff have an obligation to report any actual or suspected Personal Data breach immediately.

A Personal Data breach may include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Prompt reporting allows Smile to:

- contain and investigate the breach;
- take remedial action;
- assess risks to affected individuals;
- maintain appropriate breach records; and
- make any notifications required under Data Protection Laws.



Smile Education Limited's procedure

1. As soon as an actual or suspected Personal Data breach is identified, the employee must notify the DPO, Mark Davis, immediately.
2. The employee must preserve relevant information and make any required internal record of the incident in accordance with Smile's procedures.
3. The DPO will ensure that the breach is appropriately documented and will notify the Directors and other relevant personnel.
4. Smile will assess the nature and seriousness of the breach, the Personal Data affected and the potential consequences for individuals.
5. Where required by Data Protection Laws, Smile will notify the Information Commissioner's Office within the applicable statutory timeframe.
6. Where required, affected individuals will also be notified.
7. The DPO will record the investigation, decisions and remedial actions taken.

22. MONITORING

Everyone covered by this policy must comply with it.

The DPO, Mark Davis, has overall responsibility for monitoring this policy and will review it periodically to ensure it remains appropriate and is being followed.

This policy should also be reviewed following significant changes to Data Protection Laws, regulatory guidance, Smile's business activities or its processing of Personal Data.

23. CONSEQUENCES OF FAILING TO COMPLY

Smile takes compliance with this policy seriously. Failure to comply may put individuals and the organisation at risk.

Failure to comply with this policy may result in disciplinary action in accordance with Smile's applicable procedures and, in serious cases, may result in dismissal.

Any questions or concerns about this policy or the processing of Personal Data should be raised with the Data Protection Officer, Mark Davis.