Title	Data Protection and Privacy Policy
Cross References	**External:** • UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • Data (Use and Access) Act 2025 • Privacy and Electronic Communications Regulations 2023 • DfE Data Protection in Schools guidance (Current July 2026 edition) • ICO UK GDPR and data protection guidance **Internal:** Data Breach Policy Information Right Policy Confidentiality Policy Clear Desk and Screen Policy Online Safety Policy AI Policy AI Misuse Policy Child Protection and Safeguarding Policy Safer Recruitment Policy Lone and Home Worker Policy Complaints Policy and Procedure Records Retention Policy and Retention Schedule Information Security / IT Security Policy
Date	**October 2026**

1. Policy Statement

Apricot Online Ltd is committed to protecting the privacy, dignity and information rights of students, parents and carers, staff, applicants, contractors, commissioners and other individuals whose personal data we process. We recognise that much of the information we handle relates to children, young people and vulnerable individuals and may include safeguarding, health, SEND and other highly sensitive information.

Apricot will process personal data lawfully, fairly, transparently and securely. We will collect only the information we need, use it for clear and legitimate purposes, keep it accurate, retain it only for as long as necessary and protect it from unauthorised or unlawful access, loss, alteration, disclosure or destruction.

This policy provides the overarching framework for data protection and privacy across Apricot Online and should be read alongside the Information Rights Policy, Data Breach Policy, Confidentiality Policy and other linked information-governance policies and procedures.

2. Scope

This policy applies to all personal data processed by or on behalf of Apricot Online Ltd, whether held electronically, in cloud-based systems, in email, in lesson recordings, in documents, on portable devices, in paper records or in any other format.

It applies to directors, employees, teachers, contractors, consultants, volunteers and any other person who is given access to Apricot information or systems. Everyone handling personal data is responsible for following this policy and the related procedures relevant to their role.

3. Roles and Responsibilities

3.1 Apricot Online Ltd

Apricot Online Ltd will normally act as a data controller where it determines why and how personal data is processed for its own organisational purposes. In some commissioned arrangements Apricot may act as a data processor, or may have separate or joint controller responsibilities, depending on the service, contract and decisions made by the parties. Responsibilities should be made clear in commissioning and data-sharing arrangements rather than assumed from the name of the organisation.

3.2 Operations Director / Data Protection Lead

The Operations Director has operational oversight of data protection within Apricot and is the principal internal contact for data-protection queries, information-rights requests, complaints and significant information-governance concerns. Specialist external advice will be obtained where required. Where the law requires a formally appointed Data Protection Officer for a particular arrangement, Apricot will ensure that the role is appointed and able to act independently.

3.3 All staff and contractors

- handle personal data only where required for legitimate work purposes;
- use approved systems, accounts and storage locations;
- follow confidentiality, access-control and security requirements;
- complete required data-protection and information-security training;
- keep information accurate and report known inaccuracies;
- share personal data only with authorised recipients and only to the extent necessary;
- report suspected or actual data breaches immediately under the Data Breach Policy; and
- raise concerns if a proposed use of personal data appears excessive, unclear, insecure or outside the expected purpose.

4. Data Protection Principles

Apricot will apply the data-protection principles to all processing. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed in a way that ensures appropriate security, confidentiality, integrity and availability; and
- managed in a way that allows Apricot to demonstrate accountability and compliance.

5. Personal Data We May Process
The information Apricot processes depends on the relationship and commissioned service. It may include:

- identification and contact details;
- parent/carer and emergency contact information;
- education history, attainment, assessment, attendance and engagement information;
- SEND information, EHCP information and reasonable-adjustment requirements;
- health, medical, disability and wellbeing information relevant to education or safeguarding;
- safeguarding, child-protection, risk and welfare information;
- behaviour and incident information;
- lesson communications, submitted work and, where applicable, recordings made under approved arrangements;
- account, device, access, audit and security information generated by Apricot systems;
- commissioning, contractual and invoicing information;
- staff, applicant, contractor and safer-recruitment information, including criminal-offence information where legally permitted; and
- any other information reasonably required to provide, administer, secure or evaluate Apricot services.

6. Special Category and Criminal Offence Data
Apricot regularly handles information that receives additional protection under data-protection law, including health information and data revealing racial or ethnic origin, religious or philosophical beliefs, sexual orientation or other special category information. Safeguarding and recruitment processes may also involve criminal-offence data.

Where special category data is processed, Apricot will identify both a lawful basis for the processing and an additional condition permitting the use of that sensitive information. Criminal-offence data will be processed only where the law allows and with appropriate safeguards. Access will be restricted to those who need the information for their role.

7. Lawful Bases for Processing
A lawful basis must be identified for each processing activity. The most appropriate basis depends on why the information is being used and Apricot will not rely on consent simply because it appears convenient.
Depending on the activity, Apricot may process personal data because:

- processing is necessary to comply with a legal obligation;
- processing is necessary for the performance of a contract or to take steps before entering into a contract;
- processing is necessary for a task carried out in the public interest where that basis properly applies to the arrangement;
- processing is necessary to protect the vital interests of an individual;
- Apricot has a legitimate interest which is not overridden by the rights and interests of the individual; or
- the individual has given valid consent for a specific purpose where consent is the appropriate legal basis.
- Where Apricot acts as a processor for a commissioner, personal data will be processed only on the documented instructions of the controller except where the law requires otherwise.

8. Children and Young People
Children and young people require particular care because they may be less aware of how their information is used and of the risks associated with processing. Apricot will provide privacy information in a clear and accessible way and will consider the age, understanding and best interests of the student when designing or changing processing that affects them.

Where a new technology, platform or activity is likely to create a high risk to the rights and freedoms of children or other individuals, Apricot will undertake a Data Protection Impact Assessment (DPIA) before the processing begins and will build appropriate safeguards into the design.

9. Transparency and Privacy Notices
Individuals must be told, in a clear and appropriate way, how Apricot uses their personal information. Apricot will maintain privacy notices for the relevant groups it deals with, which may include students and parents/carers, employees, applicants and contractors.

Privacy information will explain, as appropriate, what data is collected, the purposes and lawful bases, who information may be shared with, how long it is retained, relevant rights, contact details and how to raise a concern or complaint.

Where the way Apricot uses information changes materially, the relevant privacy information will be reviewed and updated.

10. Data Minimisation, Accuracy and Access
Apricot will collect and use only the personal data reasonably required for the relevant purpose. Staff should avoid collecting information "just in case" and should not copy or circulate complete records where a smaller amount of information would meet the need.

Reasonable steps will be taken to keep records accurate and up to date. Individuals should be able to correct inaccurate information through the arrangements in the Information Rights Policy.

Access to systems and records will be based on role and need. Staff should have the minimum level of access necessary to carry out their duties. Access will be reviewed when roles change and removed promptly when employment, contracts or other access requirements end.

11. Information Sharing
Apricot may need to share personal data with commissioning schools or local authorities, parents/carers, education professionals, examination or awarding bodies, safeguarding partners, health or social-care professionals, regulators, professional advisers, service providers and other organisations where there is a lawful and legitimate reason to do so.
Before sharing personal data, staff should consider whether:

- there is a clear purpose and lawful basis for the sharing;
- only the minimum necessary information is being shared;
- the recipient is authorised and the contact details are correct;
- the method of transfer is secure and appropriate to the sensitivity of the information;
- any relevant contract, data-processing agreement or data-sharing arrangement is in place; and
- the sharing creates a safeguarding issue or another risk that requires escalation.

Data protection law does not prevent proportionate information sharing for safeguarding where sharing is lawful and necessary. Staff must follow the Child Protection and Safeguarding Policy and should seek advice where uncertain rather than delaying an urgent safeguarding response.

12. Suppliers, Processors and Educational Technology

Where Apricot uses an external provider to process personal data on its behalf, due diligence will be undertaken before access to personal data is permitted. Contracts or other legally binding arrangements will include appropriate data-protection terms, including instructions, confidentiality, security, sub-processing, assistance with rights and breaches, deletion/return of data and audit or assurance arrangements as appropriate.

EdTech, learning platforms, communication tools and other digital services should be assessed for privacy and security before adoption. The amount and type of student data shared should be limited to what is needed for the service.

13. Artificial Intelligence and Automated Processing

Personal data must not be entered into public or unapproved AI tools. Any approved use of AI involving personal data must comply with the Artificial Intelligence (AI) Policy, security requirements and relevant privacy information.

Where Apricot proposes automated processing that could make, or materially contribute to, decisions with legal or similarly significant effects on an individual, the lawful basis, safeguards, transparency requirements and need for a DPIA will be considered before the processing begins. Human review and a route to challenge a significant automated decision will be provided where required by law.

14. Security of Personal Data

Apricot will use proportionate technical and organisational measures to protect personal data. These include, as appropriate:

- approved accounts and systems, strong passwords and multi-factor authentication where available;
- role-based access controls and timely removal of access;
- secure cloud storage and controlled sharing permissions;
- encryption and secure configuration of devices and storage where appropriate;
- clear desk and screen practices;
- secure disposal of paper and electronic information;
- phishing, malware and cyber-security awareness;
- backups and recovery arrangements appropriate to critical information;
- logging, monitoring and investigation of suspected unauthorised access; and
- staff training and prompt reporting of security incidents.

Detailed controls are set out in the Clear Desk and Screen Policy, Online Safety Policy, Data Breach Policy and the Information Security / IT Security Policy once adopted.

15. Lesson Recordings, Images and Communications
Where online lessons or meetings are recorded, the purpose of recording, access arrangements, security and retention must be clear. Recordings made for safeguarding, quality assurance or another approved operational purpose must not automatically be used for marketing or publicity. Any separate publicity or promotional use must have an appropriate lawful basis and follow relevant consent/permission and privacy arrangements.

Staff must use approved Apricot communication routes and must not move student information to personal email, messaging, storage or social-media accounts.

16. Retention and Disposal
Personal data will not be retained indefinitely simply because storage is available. Apricot will maintain a Records Retention Policy and Retention Schedule setting out appropriate retention periods for key record types, taking account of statutory requirements, safeguarding needs, limitation periods, contractual obligations and operational requirements.

At the end of the applicable retention period, records will be securely deleted, destroyed or anonymised unless there is a lawful reason to retain them for longer, such as an ongoing safeguarding matter, legal claim, regulatory requirement or preservation instruction.

17. Individual Information Rights
Individuals have rights in relation to their personal data. Depending on the circumstances these include rights of access, rectification, erasure, restriction, objection, portability and rights relating to certain automated decisions.

The detailed process for exercising these rights, including Subject Access Requests and identity verification, is set out in the Information Rights Policy. Requests must be passed promptly to the Operations Director / Data Protection Lead so that statutory timescales can be met.

Rights are not absolute. Where an exemption or restriction applies, Apricot will consider it carefully and explain the position where the law permits.

18. Data Protection Complaints
Apricot will provide a clear route for individuals to complain about how their personal data has been handled. A data-protection complaint should be sent to the Operations Director / Data Protection Lead. Complaints may also be raised through an accessible electronic route provided by Apricot.

Receipt of a data-protection complaint will be acknowledged within 30 days. Apricot will take appropriate steps to investigate the complaint without undue delay, keep the complainant informed as appropriate and communicate the outcome without undue delay.

If the individual remains dissatisfied, they may raise the matter with the Information Commissioner's Office. Apricot will provide appropriate information about this route in its privacy information and complaint responses.

19. Personal Data Breaches
Any actual or suspected loss, unauthorised disclosure, access, alteration, destruction or other compromise of personal data must be reported immediately under the Data Breach Policy. Staff must not delay reporting while attempting to decide whether an incident is serious enough to count as a breach.

Apricot will assess the risk to individuals, contain and investigate the incident, keep required records and make notifications to the ICO and/or affected individuals where legally required.

20. International Transfers
Where personal data is transferred or made accessible outside the United Kingdom, Apricot will ensure that an appropriate lawful transfer mechanism and safeguards are in place before the transfer occurs. The location of cloud hosting, support access and sub-processors will be considered when procuring digital services.

21. Training, Monitoring and Accountability
Staff who handle personal data will receive data-protection and information-security training appropriate to their role, with updates where legislation, technology or identified risks change.

Apricot will maintain appropriate evidence of compliance, which may include privacy notices, processing records, contracts, data-sharing agreements, DPIAs, breach records, information-rights records, training records, risk assessments and retention arrangements.

Data-protection compliance will be considered when new systems, services, technologies or significant changes to processing are introduced. Privacy and security should be designed into new arrangements rather than added after implementation.

22. Non-Compliance
A failure to follow this policy may create risks for individuals and for Apricot. Concerns will be addressed proportionately and may result in additional training, restriction of access, contractual action or action under the Employee Handbook - Disciplinary Procedure, depending on the circumstances. Serious or deliberate misuse of personal data may also require external reporting.

23. Review
This policy will be reviewed annually and sooner where changes to data-protection law, ICO or DfE guidance, Apricot systems, commissioning arrangements or identified risks make this necessary.

Authorised by: Jodie Phillips, Operations Director

Date: October 2026

Review Date: October 2027