Title	**Information Security and IT Security Policy**
Cross References	**External:** • **UK General Data Protection Regulation (UK GDPR)** • **Data Protection Act 2018** • **Data (Use and Access) Act 2025** • **DfE Cyber Security Standards for Schools and Colleges** • **DfE Data Protection in Schools Guidance** • **National Cyber Security Centre (NCSC) guidance** **Internal:** Data Protection and Privacy Policy Data Breach Policy Records Retention Policy and Retention Schedule Staff Acceptable Use Agreement Online Safety Policy Clear Desk and Screen Policy Confidentially Policy Lone and Home Worker Policy AI Policy Virtual Lessons and Online Meetings Procedure Child Protection and Safeguarding Meeting Business Continuity Arrangements
Date	**October 2026**

1. Policy Statement

Apricot Online Ltd is dependent on secure and reliable digital systems to deliver online alternative provision, communicate with students and commissioners, safeguard children and young people, manage staff and operate the organisation. Information security is therefore an organisational, safeguarding and data-protection responsibility, not solely a technical issue.

Apricot will take proportionate technical and organisational measures to protect the confidentiality, integrity and availability of its information, systems and services. Security controls will reflect the nature of Apricot's online operating model, the sensitivity of the information processed and the risks associated with remote access, cloud services and work involving children and young people.

2. Scope

This policy applies to Apricot information, systems, accounts, devices, networks, cloud services, learning platforms, communication tools, records and other digital resources. It applies to directors, employees, teachers, contractors, consultants and other authorised users, including those working remotely or using an authorised personal device.

Third-party providers that process Apricot information or provide critical digital services must also meet appropriate contractual, privacy and security requirements.

3. Security Objectives

Apricot's information-security arrangements are designed to:

- protect confidential and personal information from unauthorised access, disclosure, alteration or loss;
- ensure information remains accurate, complete and trustworthy;
- maintain access to critical systems and information when required;
- reduce the likelihood and impact of cyber attack, phishing, malware, account compromise and accidental disclosure;
- protect students, staff, commissioners and the organisation from harm caused by misuse of information or systems;
- support safeguarding, data-protection and contractual obligations; and
- enable Apricot to detect, respond to and recover from security incidents.

4. Governance and Responsibilities

4.1 Managing Director

The Managing Director has overall operational responsibility for information security, including ensuring that appropriate policies, access controls, incident arrangements, staff expectations and supplier controls are in place. Technical advice and specialist support will be obtained where required.

4.2 System and service owners

Those responsible for systems or services must ensure that access is appropriate, security settings are reviewed, supplier information is considered, important changes are controlled and identified risks are escalated.

4.3 All users

All authorised users are responsible for following the Staff Acceptable Use Agreement and relevant Apricot policies, protecting their accounts and devices, handling information securely and reporting concerns promptly.

5. Risk Management

Information-security risks will be considered as part of Apricot's wider risk-management arrangements. Risk assessments should consider the sensitivity of the information involved, number and type of individuals affected, likelihood of compromise, impact on education or safeguarding, dependence on the service and available controls.

Significant new systems, services or changes to processing should be assessed before implementation. Where personal-data processing is likely to result in a high risk to individuals, a Data Protection Impact Assessment (DPIA) will be completed in accordance with the Data Protection and Privacy Policy.

6. Account and Access Management

Access to Apricot systems will be based on role and legitimate business need.

- Each user should have an individual account wherever the system supports this.
- Shared accounts should be avoided unless there is a documented operational reason and appropriate control.
- Users must not share passwords or authentication codes.
- Multi-factor authentication should be enabled for important cloud, email, administrative and other supported accounts wherever reasonably available.
- Administrative or elevated privileges must be limited to those who require them.

- Access permissions should follow the principle of least privilege.
- Access will be reviewed when roles change and removed promptly when employment, engagement or other authority ends.
- Dormant or unnecessary accounts should be disabled or removed.
- Suspected account compromise must be reported immediately.

7. Passwords and Authentication

Passwords must be strong, difficult to guess and not reused across unrelated personal and Apricot services. Passwords must not be written or stored in an insecure location or sent through insecure channels.

Where a password manager or other credential-management solution is approved by Apricot, it should be used in accordance with the relevant instructions. Users must never approve an unexpected multi-factor authentication request.

8. Devices

Devices used to access Apricot systems must be reasonably secured and maintained.

- Devices must be protected by a password, PIN, biometric control or equivalent.
- Supported operating systems, browsers and applications should be kept up to date.
- Automatic security updates should be enabled where appropriate.
- Anti-malware and built-in security protections should be active where supported.
- Devices should automatically lock after a reasonable period of inactivity.
- Apricot information must not be left visible or accessible to family members or other unauthorised people.
- Lost or stolen devices that contain or can access Apricot information must be reported immediately.
- Sensitive Apricot information should not be permanently stored on a personal device unless specifically authorised and appropriately protected.

9. Patch and Vulnerability Management

Security updates and patches should be applied within a timescale proportionate to the risk. Critical or actively exploited vulnerabilities affecting Apricot's systems or services should be addressed as a priority.

Unsupported software, operating systems or services should not be relied upon for Apricot work where they no longer receive appropriate security updates. Where an immediate replacement is not possible, the risk and temporary controls should be documented.

10. Email, Phishing and Malicious Content

Email remains a significant route for fraud, malware and account compromise. Users must remain alert to unexpected messages, urgent requests, unusual payment instructions, links, attachments and requests for passwords or authentication codes.

- Suspicious links or attachments should not be opened.
- Requests involving payments, bank details, passwords or sensitive information should be independently verified where unusual or unexpected.
- Users should report suspected phishing or impersonation promptly.
- A user who has clicked a suspicious link or entered credentials must report this immediately rather than waiting to see whether harm occurs.
- Email forwarding to personal accounts is not permitted for Apricot confidential or student information.

11. Cloud Services and Approved Systems
Apricot primarily operates through cloud-based services. Personal, safeguarding or confidential information must therefore be stored and processed only in systems approved for the relevant purpose.

Before a new cloud service, learning platform, communication tool or other supplier is adopted, Apricot should consider:

- the information the service will process;
- security and access controls;
- data-protection roles and contractual terms;
- hosting and international transfer arrangements;
- sub-processors and third-party access;
- backup, resilience and recovery arrangements;
- incident notification arrangements;
- data export, deletion and termination arrangements; and
- whether a DPIA or additional risk assessment is required.

12. Personal Devices and Remote Working
Where authorised personal devices are used for Apricot work, the same confidentiality, access and security standards apply. Staff must follow the Staff Acceptable Use Agreement, Lone and Home Working Policy and Clear Desk and Screen Policy.

Apricot records should remain within approved cloud systems rather than being routinely downloaded to personal devices. Where temporary local access is necessary, copies should be removed when no longer required and should not be backed up into personal cloud accounts.

13. Data Sharing and Secure Transfer
Confidential and personal information must be shared only with authorised recipients and by an appropriately secure method. Staff must check recipient details before sending information and should use the minimum data necessary.

Highly sensitive information should not be sent through an insecure route merely for convenience. Where secure portals, controlled links, restricted permissions or encryption are available and appropriate, these should be used.

14. Backups, Resilience and Recovery
Apricot will maintain appropriate backup and recovery arrangements for critical information and services, taking account of the facilities provided by its cloud suppliers.

- Critical data and systems should be identified.
- Backup or recovery arrangements should not depend on a single uncontrolled copy.
- Backups should be protected from unauthorised access and, where reasonably possible, from the same compromise that affects live data.
- Recovery arrangements should be tested or otherwise assured periodically.
- Backup retention should align with the Records Retention Policy and Retention Schedule.
- Restoration of deleted personal data from backup should occur only for legitimate recovery purposes.

15. Business Continuity
Information security includes the ability to continue or restore essential operations following a cyber incident, service outage, loss of access or other disruption. Apricot will maintain proportionate business-continuity arrangements for critical services and identify alternative communication or working arrangements where appropriate.

Significant outages affecting education delivery, safeguarding or access to critical records must be escalated promptly.

16. Logging and Monitoring
Apricot may use system logs, audit information and proportionate monitoring to protect systems, investigate incidents, administer services, support safeguarding and demonstrate compliance. Access to logs will be restricted. Logs containing personal data will be retained only for a justified period in accordance with the Records Retention Policy and Retention Schedule. Monitoring will be carried out lawfully and transparently in accordance with relevant privacy information.

17. Artificial Intelligence and Emerging Technology
Personal, safeguarding, confidential or commercially sensitive Apricot information must not be entered into public or unapproved AI tools. Approved AI use must follow the Artificial Intelligence (AI) Policy and Staff Acceptable Use Agreement.

New AI-enabled services should be assessed for data use, security, supplier access, model training, retention, international transfers and the ability to delete or retrieve information before confidential Apricot data is used.

18. Removable Media and Downloads
The use of removable media should be minimised. Unknown USB devices or storage media must not be connected to devices used for Apricot work. Where removable storage is necessary for confidential information, it must be authorised and appropriately secured.

Downloads containing personal or confidential information should be avoided where the information can be safely accessed in the approved cloud service. Temporary downloads must be deleted when no longer required.

19. Security Incidents and Personal Data Breaches
Any actual or suspected cyber-security incident, unauthorised access, phishing compromise, malware infection, lost device, disclosure to the wrong recipient, compromised account or other security concern must be reported immediately.

Where personal data may be affected, the Data Breach Policy applies. Staff must not delay reporting while attempting to determine whether the incident is serious enough to notify externally.

Apricot will contain, assess, investigate and document significant incidents and will make regulatory, safeguarding, contractual or other notifications where required.

20. Safeguarding
A cyber-security or online incident may also be a safeguarding incident. Where an event involves harmful contact, exploitation, inappropriate material, student account misuse, threats, coercion or another concern about a child or vulnerable person, staff must follow the Child Protection and Safeguarding Policy in addition to reporting the technical incident.

Technical investigation must not delay urgent action required to protect a child.

21. Supplier and Contractor Security
Suppliers and contractors with access to Apricot systems or information must be subject to proportionate due diligence and contractual controls. Access should be limited to what is required for the service and removed when no longer necessary.

Apricot should consider relevant supplier assurance, security certifications, incident history, contractual commitments and the criticality of the service rather than relying solely on marketing claims.

22. Records Retention and Secure Disposal
Information must be retained and securely disposed of in accordance with the Records Retention Policy and Retention Schedule. Devices and storage media must be securely wiped, sanitised or destroyed before disposal or reuse where they have contained confidential Apricot information.

23. Security Awareness and Training
Staff and contractors will receive information-security and data-protection training appropriate to their role. Training will include, as relevant, password security, multi-factor authentication, phishing, data handling, remote working, safeguarding, incident reporting and use of AI.

Apricot may issue additional alerts or guidance where new threats, vulnerabilities or working practices create a material risk.

24. Compliance and Review
Failure to follow this policy may result in restriction or removal of access, additional training, contractual action or action under the Employee Handbook – Disciplinary Procedure, depending on the circumstances.

This policy will be reviewed annually and sooner following a significant security incident, material change in Apricot systems, new legal or regulatory requirements or significant changes in cyber-security risk.

Authorised by: Jodie Phillips, Operations Director

Date: October 2026

Review Date: October 2027