Title	Data Breach Policy
Cross References	**Internal:** Data Protection and Privacy Policy Child Protection and Safeguarding Policy Whistleblowing Policy Confidentiality Policy Restrictive Covenant Agreement AI Policy Online Safety Policy
Date	**October 2026**

1. Introduction

Apricot Online collects, uses, stores and shares personal data in order to provide its services and meet its legal, contractual and safeguarding responsibilities. Personal data is a valuable asset and must be protected appropriately.

Apricot Online is committed to maintaining the confidentiality, integrity and availability of personal data and to responding promptly and effectively to any actual or suspected personal data breach.

A personal data breach may result in harm to individuals, disruption to services, reputational damage, regulatory action and financial loss. All staff must therefore understand how to recognise, report and respond to a suspected breach.

2. Purpose and Scope

This policy sets out Apricot Online's arrangements for identifying, reporting, containing, investigating, assessing and recording personal data breaches in accordance with applicable UK data protection legislation, including the UK GDPR and Data Protection Act 2018.

It applies to all personal data processed by or on behalf of Apricot Online, regardless of format or location, including information held in electronic systems, cloud services, email, paper records, portable devices and other approved systems.

This policy applies to all employees, workers, contractors and others who process personal data on behalf of Apricot Online. Students should report any suspected data security incident to an appropriate member of staff.

The objectives of this policy are to:

- contain breaches and reduce their impact as quickly as possible;
- protect affected individuals and Apricot Online;
- ensure appropriate investigation and risk assessment;
- meet legal and contractual notification requirements;
- maintain an accurate record of breaches and decisions; and
- identify lessons learned and reduce the likelihood of recurrence.

3. Definition and Types of Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

For the purposes of this policy, staff must report both confirmed and suspected breaches. Examples include, but are not limited to:

- sending an email, attachment or message containing personal data to the wrong recipient;
- using an incorrect email distribution list or exposing recipients' email addresses inappropriately;
- incorrect file, folder, cloud-storage or document-sharing permissions;
- loss or theft of a laptop, phone, tablet, USB device or paper record containing personal data;
- loss, accidental deletion or unauthorised alteration of personal data;
- unauthorised access to an account, system, mailbox or document;
- phishing, credential compromise, malware, ransomware, hacking or other cyber-security incidents affecting personal data;
- disclosure of confidential or special category data to an unauthorised person;
- paperwork or information being left where it can be viewed or accessed by unauthorised people;
- failure of systems or equipment resulting in loss of availability or access to personal data;
- accidental publication of personal data on a website or other public platform;
- verbal disclosure of personal data to an unauthorised person; and
- deception or social engineering used to obtain personal information.
- Not every information-security incident will amount to a personal data breach, but any incident involving or potentially involving personal data must be reported promptly so that it can be assessed.

4. Immediate Reporting

Any person who becomes aware of an actual or suspected personal data breach must report it immediately to the Operations Director and/or the designated Data Protection Lead using Apricot Online's usual internal reporting route. Staff must not delay reporting while attempting to investigate the incident themselves.

If an incident is discovered outside normal working hours, it must be escalated as soon as reasonably practicable. Where the incident is ongoing or presents an immediate risk, reasonable steps should be taken to prevent further disclosure or loss without compromising evidence or security.

The initial report should include, where known:

- the date and time the incident occurred and was discovered;
- the person reporting it and their contact details;
- a clear description of what happened;
- the systems, devices, records or services involved;
- the type of personal data involved;
- the approximate number and categories of individuals affected;
- whether children or other potentially vulnerable individuals are affected;
- who may have received or accessed the data; and
- any immediate action already taken.

The Data Breach Report Form at Appendix 1 should be completed as soon as practicable. Failure by staff to report or appropriately manage a breach may be addressed under relevant disciplinary procedures.

5. Containment and Recovery

The Operations Director, Data Protection Lead or nominated Lead Investigation Officer will establish whether the breach is continuing and coordinate immediate containment.

Depending on the circumstances, containment may include:

- recalling or requesting deletion of a misdirected email or document;
- removing or correcting sharing permissions;
- resetting passwords, disabling accounts or revoking sessions;
- isolating affected devices or systems and obtaining appropriate IT support;
- recovering lost data from secure backups;
- contacting an unintended recipient and obtaining confirmation that information has been securely deleted;
- preserving relevant evidence and audit logs; and
- taking steps to protect individuals from foreseeable harm.

External specialist advice, insurers, service providers, law enforcement or other relevant bodies may be contacted where appropriate.

6. Investigation and Risk Assessment

An investigation will begin without undue delay. Wherever practicable, an initial assessment should be completed promptly so that any required regulatory notification can be made within the applicable legal timeframe.

The investigation will establish the facts and assess the likelihood and severity of risk to the rights and freedoms of affected individuals. Factors to consider include:

- the nature, sensitivity and volume of the personal data involved;
- whether special category data, criminal offence data, safeguarding information, financial information or identity documents are involved;
- whether children or other vulnerable individuals are affected;
- the number and categories of individuals and records affected;
- whether the data was encrypted, pseudonymised or otherwise protected;
- whether the data has been recovered, deleted or confirmed as inaccessible;
- the identity and trustworthiness of any unintended recipient;
- the likelihood of further disclosure or misuse;
- possible consequences including distress, discrimination, identity theft, fraud, reputational damage, safeguarding risk or loss of confidentiality;
- the duration of the breach and whether it is ongoing; and
- any contractual, safeguarding or other regulatory implications.

The assessment and the reasons for the decision reached must be recorded, including where Apricot Online decides that notification to the Information Commissioner's Office (ICO) or affected individuals is not required.

7. Notification to the ICO

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, Apricot Online will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

The 72-hour period runs from the point at which Apricot Online becomes aware that a personal data breach has occurred. A notification should not be delayed simply because every fact is not yet known; information may be provided in phases where necessary.

A notification to the ICO will include, where available:

- a description of the nature of the breach;
- the categories and approximate number of affected individuals;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the Data Protection Officer, where appointed, or other appropriate contact point;
- the likely consequences of the breach; and
- the measures taken or proposed to address the breach and mitigate its effects.

Where a breach is reported later than 72 hours, the reasons for the delay will be documented and provided where required.

8. Notification to Affected Individuals

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, Apricot Online will inform those individuals without undue delay unless a lawful exception applies.

Communications will be clear and in plain language and will normally include:

- a description of the nature of the breach;
- the name and contact details of an appropriate contact point;
- the likely consequences of the breach;
- the measures taken or proposed to address the breach and mitigate possible adverse effects; and
- practical advice on steps the individual can take to protect themselves, where relevant.

When affected individuals are children, Apricot Online will consider the most appropriate method of communication, including whether communication should be made to or through a parent/carer, commissioner or other responsible professional, taking account of safeguarding, confidentiality and the individual circumstances.

9. Other Notifications and Escalation

Depending on the nature of the incident, Apricot Online may also need to notify or liaise with commissioning organisations, relevant data controllers or processors, insurers, IT or service providers, law enforcement, safeguarding partners, banks or other regulatory or professional bodies.

Where Apricot Online is acting as a data processor and becomes aware of a personal data breach affecting data processed on behalf of a controller, the relevant controller will be informed without undue delay in accordance with contractual and legal requirements.

Any external communication or media response relating to a significant breach must be coordinated by the Operations Director or other authorised senior leader.

10. Recording Breaches

Apricot Online will maintain a record of all personal data breaches, including breaches that are not reported to the ICO.

The record will include the facts of the breach, its effects, the risk assessment, decisions regarding notification, remedial action taken and relevant communications. Where a decision is made not to notify the ICO or affected individuals, the reasons must be documented.

11. Evaluation, Lessons Learned and Prevention

Once the immediate incident has been contained, Apricot Online will review the cause of the breach, the effectiveness of the response and whether changes are required.
The review may consider:

- whether technical and organisational security measures were adequate;
- whether access permissions and account controls were appropriate;
- whether data was being stored, shared and retained appropriately;
- whether only the minimum necessary personal data was used or disclosed;
- whether staff awareness, training or supervision should be strengthened;
- whether supplier, processor or contractual arrangements require review;
- whether policies, procedures or systems should be amended; and
- whether additional monitoring, testing or audit is required.

Significant findings and recommended actions will be escalated to the Senior Leadership Team as appropriate. Actions will be assigned, monitored and reviewed to reduce the risk of recurrence.

12. Roles and Responsibilities

All staff and other authorised users

All staff and other authorised users are responsible for protecting personal data, following Apricot Online policies and reporting actual or suspected breaches immediately.

Operations Director / Data Protection Lead

The Operations Director and/or designated Data Protection Lead is responsible for coordinating the response, ensuring appropriate risk assessment and documentation, determining whether specialist advice is required and ensuring that legal or contractual notifications are considered.

Lead Investigation Officer

A Lead Investigation Officer may be appointed for an incident where appropriate. The person appointed will coordinate fact-finding, containment, evidence gathering and recommended remedial action, reporting to the Operations Director/Data Protection Lead.

Senior Leadership Team

The Senior Leadership Team will support implementation of corrective action and consider significant organisational learning arising from serious or repeated incidents.

13. Policy Review

This policy will be reviewed annually and sooner where there are significant changes to legislation, regulatory guidance, technology, organisational practice or following a significant data breach.

APPENDIX 1 - DATA BREACH REPORT FORM

Act promptly. Report an actual or suspected breach immediately to the Operations Director and/or designated Data Protection Lead. Complete this form as soon as practicable; do not delay the initial report while waiting to complete the form.

Section 1 - Initial Notification	
Date and time incident discovered:	
Date and time incident occurred (if known):	
Name and contact details of person reporting:	
Location / system / service involved:	
Brief description of incident:	
Type of personal data involved:	
Approximate number of individuals affected:	
Are children or vulnerable individuals affected? If yes, give details:	
Who may have received/accessed the data?	
Immediate action taken:	
Section 2 - Investigation and Risk Assessment	
Lead Investigation Officer / person completing assessment:	
Systems, equipment, accounts or records involved:	
Categories and approximate number of records affected:	
Nature and sensitivity of data, including any special category / criminal offence / safeguarding / financial data:	
Security measures in place (e.g. encryption, access controls):	
Has the data been recovered, deleted or contained? Evidence obtained:	
Likely consequences for affected individuals:	
Likelihood of harm: Low / Medium / High	
Severity of harm: Low / Medium / High	
Overall risk to rights and freedoms and rationale:	
Is the breach likely to result in a risk to rights and freedoms? Yes / No	
Is the breach likely to result in a HIGH risk to rights and freedoms? Yes / No	
Other legal, safeguarding, contractual or regulatory considerations:	

Section 3 - Action and Notifications	
Incident reference number:	
Containment / recovery action taken:	
Further action required and responsible person:	
ICO notification required? Yes / No. Rationale:	
If ICO notified: date/time and reference:	
If not notified to ICO: reason recorded:	
Affected individuals must be informed? Yes / No. Rationale:	
If individuals informed: date/method:	
Controller / commissioner / processor notification required? Details:	
Other external notifications (e.g. police, insurer, safeguarding partner):	
Lessons learned / changes required:	
Date incident closed:	
Closed / authorised by:	

Authorised by: Jodie Phillips, Operations Director

Date: October 2026

Review Date: October 2027