

Title	Clear Desk and Screen Policy
Cross References	Internal:  Data Protection and Privacy Policy  Complaints Policy  Data Breach Policy  Information Security Policy
Date	October 2026

1. Introduction

Apricot Online takes the security and confidentiality of personal data and other sensitive information seriously. This policy supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and Apricot Online's wider data protection and information security arrangements. Information is a valuable organisational asset and must be protected from loss, theft, damage, accidental disclosure and unauthorised access. This includes information held on paper, electronically, in email or cloud-based systems, on portable devices and in visual, audio or video formats.

Personal data includes information relating to an identified or identifiable living individual. Apricot Online handles personal data relating to students, parents/carers, employees, contractors, commissioners and other individuals.

A clear desk and clear screen approach reduces the risk of confidential or personal information being viewed, accessed, lost or disclosed to people who are not authorised to see it.

2. Scope

This policy applies to all employees, contractors and other authorised users who access Apricot Online information, systems or equipment.

It applies whether work is undertaken at Apricot Online premises, at home, at another workplace, while travelling or in any other location.

The policy covers information in all relevant formats, including:

- paper records and handwritten notes;
- electronic documents, databases and cloud-based files;
- emails and approved electronic communications;
- work-related photographs, images, audio and video;
- laptops, desktop computers, tablets and mobile phones;
- portable storage devices where their use has been authorised; and
- printed material or any other record containing personal, confidential or commercially sensitive information.

3. Roles and Responsibilities

All staff are responsible for protecting the information they access or handle and for following Apricot Online's data protection, information security and safeguarding requirements.

Staff must take reasonable steps to prevent unauthorised people, including family members, visitors or members of the public, from viewing or accessing confidential information.

Managers are responsible for promoting compliance within their areas of responsibility and for raising concerns or recurring risks through the appropriate organisational route.

4. Clear Desk Procedure

Personal, confidential and commercially sensitive information must not be left unattended or visible to unauthorised people.

Staff must:

- keep paper records containing personal or confidential information secure when they are not being actively used;
- store confidential paperwork in an appropriate secure location at the end of the working day and whenever it will otherwise be left unattended for a significant period;
- avoid unnecessary printing and use electronic documents wherever appropriate;
- collect printed documents containing personal or confidential information promptly and ensure that printers are positioned or used in a way that prevents unauthorised access;
- check printers and work areas after printing, scanning or copying to ensure confidential material has not been left behind;
- dispose of confidential paper through an approved secure destruction method and never place it in ordinary household or general waste;
- keep notebooks, diaries and handwritten notes containing personal information secure;
- keep portable devices and authorised storage media secure and out of sight when not in use; and
- avoid writing passwords or access credentials on notes that are left on or near a workstation.

5. Home and Remote Working

Apricot Online operates extensively through remote and online working. The same standards of confidentiality and information security apply when staff work from home or another remote location.

When working remotely, staff must:

- choose a working position that prevents family members, visitors or others from seeing confidential information on screen or on paper;
- avoid leaving student, staff or commissioner information visible in shared household areas;
- secure paperwork and devices when work is finished or when the work area is unattended;
- ensure confidential conversations, online lessons or meetings cannot reasonably be overheard by unauthorised people;
- use Apricot Online-approved systems, accounts and storage arrangements for work information;
- avoid downloading or retaining confidential information on personal devices unless specifically authorised; and
- take particular care when printing at home and ensure any confidential waste is securely destroyed.

6. Clear Screen Procedure

Computer, tablet and mobile-device screens must be protected from unauthorised viewing and access.

Staff must:

- lock their device whenever they leave it unattended, even for a short period;
- use password, PIN, biometric or other approved device security controls;
- use automatic screen-locking or timeout settings where available and appropriate;
- position screens so that confidential information cannot readily be viewed by unauthorised people;
- close or minimise confidential documents when they are no longer required;
- log out of systems where appropriate when work has finished;
- never share passwords or authentication codes with another person; and
- take care when screen sharing during online meetings or lessons to ensure that unrelated emails, notifications, student information or other confidential material are not displayed.

Staff should use the appropriate locking function for their device and operating system rather than relying on a single keyboard shortcut.

7. Working in Public or Shared Places

Confidential work should only be undertaken in public or shared locations where privacy can be maintained. Staff must consider the risk of other people viewing screens, overhearing conversations or accessing paperwork when working on public transport, in cafés, hotels, waiting areas or other shared environments.

Where privacy cannot be adequately maintained, staff should postpone confidential work until they are in a suitable location. Confidential or safeguarding-related telephone and video conversations must not be conducted where they can readily be overheard.

8. Portable Devices and Removable Storage

Laptops, tablets, mobile phones and other portable devices used for Apricot Online work must be protected using appropriate security controls.

Removable storage devices, including USB drives and portable hard drives, should only be used where authorised and necessary. Where such devices contain personal or confidential information, appropriate encryption and security controls must be used.

Portable equipment must not be left unattended in insecure locations and should be stored securely when not in use.

9. Data Breaches and Security Incidents

Any actual or suspected loss, theft, unauthorised access, accidental disclosure or inappropriate viewing of personal or confidential information must be reported promptly in accordance with Apricot Online's Data Breach Policy.

This includes, for example, paperwork being lost, information being sent or printed to the wrong recipient, a device being lost or stolen, an unauthorised person viewing a screen, or confidential information being left accessible.

Staff must not delay reporting because they are unsure whether an incident amounts to a personal data breach. The appropriate person will assess the incident and determine what further action is required.

10. Compliance and Review

Failure to follow this policy may place students, staff and Apricot Online at risk and may be addressed under the organisation's relevant procedures.

This policy will be reviewed annually and sooner where changes to legislation, technology, working practices or identified risks make this necessary.

Authorised by: Jodie Butler, Operations Director

Date: October 2026

Review Date: October 2027