Clear Desk Policy

Policy Code:	HR35
Policy Start Date:	September 2026
Policy Review Date:	September 2029

Please read this policy in conjunction with the policies listed below:

- HR6 Data Protection Policy
- HR6A Data Breach Policy
- HR12 Staff Disciplinary Policy
- HR33 Records Management Policy

1 Policy Statement

1.1 This procedure shall apply to all staff of The Priory Federation of Academies Trust (the Trust).

1.2 This policy identifies the procedure to follow to ensure information is protected and secure.

1.3 A clear desk policy reduces the risk of data loss by ensuring no confidential information is left unattended throughout the organisation. This protects the confidentiality and integrity of information by ensuring it is not accessible to unauthorised persons outside normal working hours or when the owner of the information is not there.

1.4 References to the Trust or Academy within this policy specifically include all nursery, primary, secondary and special academies within the Trust, as well as Priory Apprenticeships and Lincolnshire ITT.

1.5 This policy does not form part of any member of staff's contract of employment and it may be amended at any time.

2 Roles, Responsibilities and Implementation

2.1 The People, Performance and Operations Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. This committee delegates day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Director of Trust Services.

2.2 This policy is approved by the People, Performance and Operations Committee before being ratified at the next available Trust Board meeting. Approval and ratification is minuted, with records kept by the Clerk to Trustees.

2.3 Leaders and managers have a specific responsibility to ensure the fair application of this policy and all staff are responsible for supporting colleagues and ensuring its success.

3 Aims

3.1 This policy aims to establish the minimum requirements for maintaining a clear desk – where sensitive/critical information about staff, students, intellectual property and contractors is placed out of site and, where possible, secure in locked areas.

3.2 The key principles of adhering to the clear desk policy are listed below:

- to reduce the risk of a security breach or information theft;

- to reduce the risk of confidential and sensitive information/documentation being stolen or accessed by unauthorised individuals which could damage the integrity of the Trust;
- to help demonstrate compliance with the Data Protection Act 2018; and
- to create a culture of staff responsibility in relation to the handling and care of personal data and other confidential information.

4 Clear Desk Procedure

4.1 Confidential and sensitive information, whether held electronically or in paper format, must be secured appropriately at the end of each working day and when staff are absent from their workplace.

4.2 In order to ensure that this is applied within the Trust, the below procedure is to be followed:

a) staff are required to ensure that all confidential and sensitive information in hardcopy or electronic form is secure in their work area at the end of the day or, if they leave their desk, at any point during the working day;
b) staff must ensure that confidential information is stored in the correct place/system, e.g., the management information system (MIS), and if notes are made in a temporary place, e.g., a notebook, the notes are transferred to the correct place in a timely manner, i.e., within one working day;
c) to reduce the risk of a breach of confidentiality and to adhere to the Data Protection Act, confidential and sensitive documents, including person identifiable information, when no longer required, must be confidentially disposed of immediately;
d) computer desktops must be logged off or have a password locked screensaver when the member of staff is away from their work area;
e) filing cabinets, office cupboards or desk drawers must be kept closed and locked when not in use, or unattended, if they contain any confidential and sensitive information;
f) keys for the locked areas must be kept out of the reach of any person(s) who are not authorised to have access to the information locked away. If the member of staff will be on annual leave or working outside the office, if appropriate, the keys should be left with a colleague in the same department;
g) when any confidential and sensitive information is requested over the phone, all staff must ensure they are speaking to the correct person to whom this information can be disclosed. This can be confirmed by calling the recipient back on a number that is already recorded in the Trust system or asking relevant questions to which the recipient would know the answer;
h) when any confidential and sensitive information is being shared staff should in the first instance make use of sharing functionality contained within Microsoft SharePoint, Teams, OneDrive etc.
i) where documents that contain confidential and sensitive information cannot be shared as above and must be sent as an attachment via email the file must be password protected. Staff should call the recipient of the email to

give the password once the document has been emailed across, or send the password in a separate email. The password must not be sent in the same email as the document;

j) when saving confidential and sensitive information to SharePoint, it is the responsibility of the member of staff to check who has access to the file/page and ensure that the information is only shared with those authorised to access the information;

k) no confidential or sensitive information is to be saved to USB drives or other external drives, even if the documents are password protected. If there is a requirement for any of this information to be saved to external drives, the member of staff is required to obtain permission from the Trust's Data Protection Officer before proceeding;

l) all staff are advised to assess whether any confidential or sensitive information needs to be printed before doing so. If it is not required to print the information, the Trust advises that the information is stored electronically. If printed, it must be stored securely and confidentially disposed of when no longer required; and

m) desks and other work spaces must be sufficiently tidy at the end of each working day to permit the Trust's cleaning staff to perform their duties, and to prevent any unauthorised individual(s) having access to confidential information.

5 Printers and Photocopiers

5.1 All Trust staff receive an access card and/or printer PUK and PIN code to enable the printing of documents through password protection. All staff must keep their codes confidential and their access card secure. If these codes/cards are shared with colleagues and a breach of confidentiality occurs, this will be dealt with through the Trust's Staff Disciplinary Policy.

5.2 When sending scanned confidential or sensitive information from the printer to an email address, all staff must send the documents from the printer to their work email address and then forward on to the required person to ensure that only the correct recipient receives the information. It is not recommended that documents are scanned and sent from the printer to the recipient directly.

5.3 If it is necessary to copy any confidential or sensitive information, the member of staff must remain at the printer whilst the copy is being completed and ensure all copies are removed from the printing tray on completion.

6 Policy Change

6.1 This policy may only be amended or withdrawn by the Priory Federation of Academies Trust.