Clear Desk Policy

Policy Code:	HR35
Policy Start Date:	September 2017
Policy Review Date:	September 2020

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

- HR6 Data Protection Policy
- HR12 Staff Disciplinary Policy

1 Policy Statement

1.1 This procedure shall apply to all employees 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 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2 Roles, Responsibilities and Implementation

2.1 The Pay, Performance and HR 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 Head of Human Resources.

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

3 Aims

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

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 1988;
- 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 when staff are absent from their workplace and at the end of each working day.

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

a) Employees 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) 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 disposed of immediately, using the Trust's shredder.
c) Computer desktops must be logged off or have a password locked screensaver when the employee is away from their work area.
d) 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.
e) Keys for the locked areas must not be left unattended at the employee's work area. All keys should remain with the employee at all times. If the employee will be on annual leave or working outside the office, if appropriate, the keys should be left with a colleague in the same department.
f) When any confidential and sensitive information is requested over the phone, all employees 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 one the recipient would know the answer.
g) Documents that contain confidential and sensitive information and which are being sent via email must be encrypted (password protected). Employees must call the recipient of the email to give the password once the document has been emailed across. The password must not be sent in the same email as the document.
h) When saving confidential and sensitive information to SharePoint, it is the responsibility of the employee to check who has access to the file and ensure that the information is only shared with those authorised to access the information.
i) No confidential or sensitive information is to be saved to USB drives or other external drives, even if the documents are encrypted (password protected). If there is a requirement for any of this information to be saved to external drives, the employee is required to obtain permission from the Trust's Data Protection Officer before proceeding.

j) All employees 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 shredded when no longer required.

k) 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.

5 Printers and Photocopiers

5.1 All Trust employees receive an access card and printer PUK and PIN code to enable the printing of documents through password protection. All employees must keep their codes confidential. If these codes 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 employees 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 employee 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

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

The Priory Federation of Academies Trust
Clear Desk Policy

This Policy has been approved by the Trust's Pay, Performance and HR Committee:

Signed…… Name..... Date:

Trustee

Signed…… Name..... Date:

Chief Executive Officer

Signed…… Name..... Date:

Designated Member of Staff

Please note that a signed copy of this agreement is available via Human Resources.