Cyber Security Policy

Policy Code:	ICT4
Policy Start Date:	September 2025
Policy Review Date:	September 2026

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

- HR5 Acceptable Use Policy
- HR6 Data Protection Policy
- HR6A Data Breach Policy
- HR22 Social Media (Staff) Policy
- HR29 Staff Code of Conduct
- HR33 Records Management Policy
- ICT2 Online Safety (Staff)
- ICT3 Online Safety (Pupils)
- Critical Incident & Business Continuity Plan

1 Policy Statement

1.1 The Trust is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out the Trust's approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and the DfE's *Keeping children safe in education* guidance.

1.2 References to the Trust or Academy within this policy specifically include all primary, secondary and special academies within the Trust, as well as the Early Years setting at the Priory Witham Academy, Priory Apprenticeships and Lincolnshire ITT.

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

1.4 This policy also applies to any third party who has access to the Trust's IT systems and data.

2 Roles, Responsibilities and Implementation

2.1 The Education & Standards 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 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.

2.3

Role	**Responsibilities**
Director of Trust Services	Overall responsibility for policy implementation and cyber security strategy.
IT Team	Implement technical controls, monitor systems, respond to incidents, manage access and updates.
Data Protection Officer	Ensure compliance with data protection law, advise on data handling, and oversee data breaches.

Role	Responsibilities
All staff	Follow this policy (and related policies), complete annual training and report incidents or concerns promptly within the setting.
Trustees	Oversee and review cyber security arrangements and policy compliance.
Governors	Support the setting with compliance with this policy, and other related policies.
Students/Staff/ Guest Users	Use IT systems responsibly, in line with ICT4 Acceptable Use Policy (AUP) and report any concerns.

3 Aims

3.1 To ensure appropriate cyber security arrangements are in place in order to reduce the risk of a cyber security incident.

4 Security Measures

4.1 The Trust implements the following security measures:

- firewalls and network security controls;
- anti-virus and anti-malware software on all devices;
- regular software updates and patch management;
- secure data backup and tested recovery procedures;
- encryption for sensitive and personal data;
- multi-factor authentication (MFA) for critical systems and remote access;
- secure configuration and monitoring of cloud services for Microsoft Office 365;
- risky user controls are in place, which will restrict any log-ins deemed to be suspicious;
- the ability for a user to be able to log-in to their account from outside the UK is disabled; and
- prompt removal of access for leavers.

4.2 The Trust is able to enforce ‘log outs’ of Microsoft accounts from devices and can also send a remote wipe which will clean any company data from the phone or personal device.

4.3 In addition to the above, the Trust will:

- only support operating systems which are fully supported with security patches by the system vendor;
- review applications annually to ensure they are safe to continue to use and are supported with security patches – if the software cannot be maintained safely then it is removed from the Trust systems or segregated;
- have an alert system in place to inform the IT Team of any critical software patches for applications and operating systems, and ensure that these are applied within 3 x weeks wherever possible;
- only support cloud systems which support multi-factor authentication; and
- review 'Privileged System Users' every 6 x months.

Anti-Malware

4.4 The Trust uses Sophos endpoint protection policies on all windows devices which are configured to protect devices and users from malware network attacks through internet activities and internet facing applications. The software is configured by the IT Infrastructure team who also monitor events highlighted by the software. The system provides alerts which are delivered to the IT Infrastructure team who action and follow up appropriately.

Firewall Exceptions

4.5 Changes to firewall rules must be recorded in a support ticket (through the Trust's internal system), follow a technical review and be approved by a Lead Infrastructure Engineer.

4.6 There are 5 stages in the Trust's firewall inbound change process:

1. Request submission – the requester submits a support ticket explaining what the need is.
2. Technical review – the IT Team will review the case and establish what IPs or Ports may need to be allowed. A security evaluation of this request will also be made at this stage including a risk evaluation
3. Approval - a Lead Infrastructure Engineer will review the case and approve or reject.
4. Testing and Implementation – a Lead Infrastructure Engineer will apply a test implementation of this and review impact, reverting if needed.
5. Closure - the original ticket will be updated with the testing/evaluation and outcome.

5 User Account Management

5.1 A user account password must have a minimum password length of at least 8 characters (with no maximum length restrictions). The Trust uses automatic blocking of common passwords using a deny list, and all staff additionally have multi-factor authentication (MFA) enabled.

5.2 For mobile devices, for example android phones and iPads a 6-digit PIN is used to unlock the device. However, even within an unlocked device, to get to business resources a username, password and MFA is required. A failed PIN will lead to a device lock-out after 4 x attempts.

5.3 Access control and permissions are based on the type of user (for example, staff, pupil, guest), job roles (where applicable) and these are reviewed regularly.

5.4 The Trust has a process in place to ensure that accounts are promptly disabled when users leave.

5.5 Account activity is monitored and audited. The Trust has an automated system which can spot unusual log-in behaviour, for example, trying lots of different passwords or logging in from unusual or impossible locations.

5.6 System Administrators are required to have a separate admin account to be used to conduct privileged activity. Privileged accounts are reviewed by a Lead Infrastructure Engineer and verified by a Senior Manager every 6 months. Access to systems and data is granted based on the principle of least privilege, IT Administrators must have had significant training (one-to-one) or experience (at least two years) before additional access is provided. System management tasks should be performed using admin accounts, not day-to-day user accounts.

5.7 Users are put into pre-defined groups to give them appropriate access to cloud and system resources, e.g., student, staff or academy groups.

6 Staff training and awareness

6.1 All staff must complete annual cyber security training, as directed by the Trust. In addition to this, the Trust carries out a cyber-attack simulation, and any user whose actions as part of the simulation are not in line with guidance and training is required to undertake additional training.

6.2 Staff training records will be kept by the setting, and will be available for inspection upon request.

7 Incident response

7.1 In the event that any user receives a suspicious email, they must not click on any links contained within the email, nor should they forward it or reply. Staff are asked to use the 'Report Message' function provided by Microsoft Outlook.

7.2 If any user is concerned that they have clicked on a suspicious link or shared information with an unverified sender, then they should report this to the IT Team immediately and then change their password for their Trust account.

7.3 If a user has any concerns or there is a suspected security incident, they must report this to the IT Team without delay, who will initiate the Cyber Response Plan, if required. If necessary, this will be dealt with as a critical incident, in line with the Trust's Critical Incident & Business Continuity Plan.

7.4 In the event that a cyber security incident involves a data breach, this will be reported to the Trust's Data Protection Officer who will work with the IT Team to manage the breach. Please see HR6A Data Breach Policy for further information.

7.5 In the event of the Trust's Cyber Response Plan being activated, a post incident evaluation will always be carried out to identify any lessons learned and update procedures if required.

8 Policy Change

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

The Priory Federation of Academies Trust

Cyber Security Policy

This Policy has been approved by the Pay, Performance & 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.