ICT Acceptable Use Policy

Policy Code:	HR5
Policy Start Date:	December 2023
Policy Review Date:	December 2026

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

- 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 Policy (Staff)
- ICT3 Online Safety Policy (Pupils)

1. Policy Statement

1.1 The Priory Federation of Academies Trust's ICT resources are provided to facilitate a person's work as a student or employee within the Trust. The Trust seeks to provide a professional working environment for its students and staff. The Trust values its ICT systems as important business and educational assets. Priory Microsoft accounts are only issued for students who are on roll or staff with a current employment contract.

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 Appendix 1 outlines the Trust's Acceptable Use Policy for students studying Digital T Levels. In addition to the Acceptable Use Policy, students must also agree to this Appendix for the duration of their course.

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. The Pay, Performance and HR Committee delegates day-to-day responsibility for operating the policy and ensuring its implementation, review and maintenance to the Strategic IT Coordinator.

2.2 Regular reviews and reports on the implementation and compliance with agreed policies and procedures will be undertaken by the IT Management committee

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

2.4 All users (students and staff) whatever technology used, wherever and whenever connected to the network have a personal responsibility to ensure that they and others, who may be responsible to them, are aware of and comply with this policy and its guidelines.

This includes users directly connected or those connecting to the network remotely.

2.5 All users are expected to be aware of UK-GDPR and the Data Protection Act 2018, which is fully adopted by the Trust

2.6 The Trust will investigate all incidents involving the potential breach of this policy. Overall responsibility for investigation is with the Chief Executive, who will notify the appropriate managers. Incidents which are found to contravene this policy will be subject to disciplinary procedures.

3. Aims

3.1 The objectives of this policy are to ensure as far as reasonably possible:

- The Priory Federation ICT systems including email and the internet ensure practices are as safe, secure and as effective as possible

- The Trust is protected from damage or liability resulting from the use of its facilities for purposes contrary to the law of the land or any agreement under which the Trust or its systems operate.

- User accounts for any Trust IT system are provided to currently employed staff or enrolled students.

4 Purpose of Use and Authorisation of Use

4.1 The Trusts ICT systems and equipment are for work related purposes. Inappropriate use could result in access being withdrawn and an investigation to determine whether disciplinary action should follow from such use.

4.2 Access to core systems and services are controlled by a unique username and password for each user. Initial default passwords issued to any user should be changed immediately following notification of account set-up. Passwords must be unique and sufficiently complex to avoid other users guessing them. Passwords should have a minimum of eight characters, including upper and lower case and a number / symbol. All staff, as well as students in Years 12 and 13, are required to use Microsoft's MFA system, using either the Microsoft Authenticator app or a text code.

4.3 Passwords must not be divulged, nor unauthorised access to accounts be permitted, to any other person. Unauthorised access to another student/staff member's account may subject both parties to

the disciplinary process. For details of the Trust's formal authorisation procedure, see Section 6.

4.4 Designated ICT staff are permitted system access at appropriate times to carry out routine and/or essential maintenance.

4.5 The academies need to collect and use certain types of information about individuals or users. This personal information will be collected and dealt with appropriately whether stored on paper, a computer database or recorded on other media. All users are expected to ensure this complies with the UK-(GDPR) and the Data Protection Act 2018.

4.6 The policies set out in this document apply to all staff members and students within the Priory Federation network. All users must correctly identify themselves at all times. A user must not pretend to be someone else, withhold their identity or tamper with audit trails.

5. BYOD (Bring your own devices) and Remote Access

5.1 Personal devices may be used on site, but must be connected to the Trust's network via the Trust's WIFI (or through an approved WIFI network at sites not currently under the Trust's network).
Users must ensure any personal devices are safe for use (e.g. not electrically dangerous, containing malware). The Trust IT system has 'on access scanning' as a security measure to protect against malware. USB storage systems are disabled by default on Trust systems.

5.2 By connecting your personal device to our network you are accepting responsibility for any interference or damage caused by your device. By connecting your mobile device to your Trust email account you are aware that the device can be wiped remotely by academy systems in the event of security breach or theft of the device. Once connected to the email system your device may have additional security policies deployed to it (e.g. unlock PIN and attachment controls).

5.3 If you use a personal device in work (e.g. Phone, tablet or camera) ensure that photos, email attachments or other documents with personal identifiers (personal data and/or special category data) on them are not stored on the device.

5.4 If photographs of staff and/or students are taken as part of work then an Academy device must be used. Photographs should only be stored on the device and not transferred onto personal devices or personal storage systems. Images and videos should be removed from the device as soon as possible and stored in Trust secure

storage systems – e.g. Sharepoint and/or OneDrive..

5.5 Staff and student users are permitted to use the Trust system remotely but must take additional measures to protect their accounts and data – such as avoiding using shared desktop sessions with other home users, using multifactor authentication and locking screens when devices are not in use.

5.6 Staff and students connecting to school systems from home must take responsibility for their own devices including regularly installing system updates and having antivirus protection in place (especially on Windows machines).

5.7 Staff are not to store personal identification data or any confidential information related to staff and students on their home devices.

5.8 Cloud storage and data loss protection – staff should ensure that information is either stored in their user area or OneDrive. Care should be taken when sharing links to OneDrive files or attachments – especially when sharing externally or to mailing groups.

5.9 Staff mobile devices – lost or stolen. In the event of a work or personal device being lost or stolen, IT Support at the local site must be informed as soon as possible so that any work data which may be stored on it can be secured or deleted.

5.10 Device security – reasonable physical security care should be taken when using devices containing personal identifiers in public places or working at home - for example ensuring that the device is in sight at all times or in a secure location. Staff should be mindful that they have access to a great deal of confidential data – such as email addresses, names, photographs, addresses and phone numbers – which should be protected.

5.11 Work or school provided devices – These devices are managed by Priory Trust systems and have additional security controls on them to protect against malware or security attacks. Only approved software can be use on these units. Devices will also have active cloud monitoring systems. However, all users should remain vigilant to security threats such as password harvesting, social engineering or fake wi-fi accounts, as there are still many security threats from internet browsing. If your work or school provided device is lost or stolen, please report to IT Support as soon as possible so it can be remotely reset.

6 Security and Privacy

6.1 The ICT systems, infrastructure and their contents are the property of

the Trust and are provided to assist the performance of your work. Users should, therefore, have no expectation of privacy in any electronic communication sent or received, whether it is of a business or personal nature.

6.2 The Trust reserves the right to monitor and occasionally intercept network traffic on all aspects of its telephone and computer systems, whether stored or in transit, under its rights in the Regulation of Investigatory Powers Act (2000). In addition, the Trust wishes to make you aware that Closed Circuit Television (CCTV) is in operation for the protection of employees and students.

6.3 Regular sweeps will be made of the ICT systems, including internet activity logs to check for inappropriate files or domain names. Where such files are located, further action as is necessary will be taken to ascertain the contents and if necessary to remove them.

Reasons for monitoring include:

- Operational effectiveness.
- To prevent a breach of the law, this policy or another Trust policy.
- Investigate a reasonable suspicion of breach of the law, this policy or another Trust policy.

6.4 Users should be aware that second and third line ICT service staff with the appropriate privilege and when occasionally required to do so, will access all files stored on a computer or personal network folder. These staff will take all reasonable steps to maintain the privacy of users.

6.5 Proxy access to staff files including emails will only be given when authorisation is obtained from the Chief Executive or other members of the Senior Leadership Team. Such action will normally only be granted in the following circumstances:

- A suspected breach of the law or serious breach of this or another Trust policy
- At the lawful request of a law enforcement agency e.g. the police or security services

6.6 All new Software on the Federation Network must be tested by IT Support prior to purchasing - this is to ensure compatibility with hardware and software systems, ensure that the appropriate licensing for the software is in place and that it is data protection and cybersecurity compliant. This includes web based software.

6.7 All managed application software will be security checked and updated once a year (if updates are available). If no updates are

available for 3 years the software will marked as a security risk and normally be retired from our systems.

6.8 Access controls to all managed systems are allocated on the basis of business need and 'Least Privilege' is always the default. Users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role. Additional privileges can be allocated to users of managed systems after formal request and approval. Access levels for key systems are reviewed and updated on an annual basis.

7 Definitions of Unacceptable Use

- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission or material with the intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of material such that this infringes the copyright or another person.
- Creation or transmission of unsolicited bulk or marketing material to users or networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe
- Deliberate unauthorised access to networked facilities or services
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    - Wasting staff effort or time unnecessarily on IT management.
    - Corrupting or destroying other users' data.
    - Violating the privacy of other users.
    - Disrupting the work of other users.
    - Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
    - Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.
    - Other misuse of network resources, such as the introduction of 'viruses' or other harmful software
- Deliberate access, promotion or distribution of harmful, unlawful or extremist internet content

- Sharing confidential or personal data with non-authorised people or storing data in an insecure way.
- Using personal devices to store images or other personal data.

8 Breaches of this Policy

8.1 Staff or students who break the Acceptable Use Policy by involvement in any of the misuses which have been mentioned above or any activities which can be reasonably considered as similar to those outlined will be subject to the misconduct procedures. In certain circumstances, the misuse by staff will be considered by the Trust as gross misconduct.

8.2 The Trust reserves the right to use the content of any employee/students electronic communication in any disciplinary process.

8.3 The Trust has a legal duty to safeguard and promote the welfare of children, young people and vulnerable adults. The Federation takes its safeguarding duties and responsibilities very seriously and we consider it to be a high priority. Therefore any material or images that amount, or appear to amount to, child abuse images, or give rise to a safeguarding children or vulnerable adults concern will be reported to the police as possession of such images or material is an offence under the Criminal Justice Act 1988 s 160.

8.4 ICT services would suspend computer and network privileges of a user pending an investigation.

8.5 Reasons for suspending individual privileges:

- To protect the integrity, security or functionality of the Trust and/or its resources or to protect the Trust from liability and/or damage its reputation
- Secure evidence of inappropriate activity
- To protect the safety or well-being of members of The Priory Federation of Academies Trust
- Upon receipt of a legally served directive of appropriate law enforcement agencies or others

Access will be promptly restored when the protections are assured, unless access is suspended as a result of investigation or formal disciplinary action.

9 Policy Change

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

The Priory Federation of Academies Trust
Acceptable Use Policy

This Policy has been approved by the Priory Federation of Academies, 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.

Appendix 1

Cyber Attack Defence Lab (Key Stage 5)

1. Purpose of the Lab

1.1 The Cyber Attack Defence Lab is designed solely for educational and defensive/offensive cybersecurity learning. Students must only use tools within the controlled, isolated environments provided. Unauthorised hacking is strictly prohibited on any platform.

2. General Behaviour Expectations

2.1 Students are expected to:

- follow staff instructions at all times;
- use equipment safely and respectfully;
- report concerns or incidents immediately;
- act ethically when using cybersecurity tools;
- work only within approved activities; and
- help each other and be aware of other students' reactions to the methods used.

3. Permitted Actions

3.1 Students may:

- use provided Kali Linux only;
- only complete approved tasks, reflecting each task's goals;
- investigate vulnerabilities solely for learning; and
- only use teaching resources supplied by staff.

4. Prohibited Actions

4.1 Students must never:

- attempt to attack real systems outside of our computing network;
- connect Kali Linux to any other network;
- use personal devices or USBs for security tools;
- download or store offensive hacking tools;
- circumvent school filters or firewalls;
- access restricted or illegal online content; and/or
- install unauthorised software.

4.2 Breaches may lead to disciplinary action and may need to be reported to the Police under the Computer Misuse Act 1990.

5. Equipment & Data Security

5.1 Students must:

- use only academy-provided Dream-quest machines;
- save work in approved locations using strict naming conventions;
- keep passwords confidential;
- never attempt to access another student's work;
- report faults immediately; and
- follow all instructions and use guides.

6. Safeguarding & Online Behaviour

6.1 Students must:

- maintain respectful communication at all times;
- never contact external individuals through lab systems;
- not access harmful, extremist, illegal, or inappropriate content; and
- report concerns to staff immediately.

7. Monitoring & Logging

7.1 All activities are monitored and logged, and screens may be viewed by staff. Logs may be used by staff for safeguarding, behaviour monitoring, or system security.

8. Legal Compliance

8.1 All activity must comply with:

- Computer Misuse Act 1990;
- UK-GDPR & Data Protection Act 2018;
- Trust safeguarding and IT policies; and
- this policy.

9. Student Declaration

9.1 Any student undertaking a Digital T Level will be asked to sign to say they have read, understood and agree to follow this policy.

9.2 Any misuse of tools or attempts to access systems without permission is strictly prohibited and illegal.

10. Computer maintenance and repair

10.1 All Cyber lab systems (Defend systems) will be reimaged 'Windows OS' with a USB image as part of the curriculum plan fortnightly.