The Priory Federation Of Academies Trust

ICT Acceptable Use Policy

Policy Code:	HR5
Policy Start Date:	January 2016
Policy Review Date:	January 2019

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

Code of Conduct
Social Media Policy

1. Policy Statement

The Priory Federation of Academies ICT resources are provided to facilitate a person's essential work as a student or employee within the Trust. The Priory Federation seeks to provide a professional working environment for its students and staff. The Trust values its ICT systems as important business assets. 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.

2. Implementation & Enforcement

The Chief Executive of the Federation has overall responsibility for the ICT network and systems security in the Federation. Specific security tasks are delegated to staff in ICT and Data Support.

2.1

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

2.2.

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.

2.3. Breach

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. Policy Details

3.1. Purpose of Use and Authorisation of Use

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 Inappropriate use could result in access being withdrawn and an investigation to determine whether disciplinary action should follow from such use.

Access to all systems and services is controlled by a central network computing account and password. Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords must be personalised and sufficiently complex to avoid other users guessing them.

Passwords must not be divulged nor access to accounts be permitted to any other person, except to designated ICT staff for system support. Unauthorised access to another staff/student member's account may subject both parties to the disciplinary process.

Personal equipment may be connected to the network via wifi and usb ports may be used for additional storage (staff only). Users must ensure these are safe for use (eg. not electrically dangerous, containing malware or any potential breach as described in 3.3).

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 Academy 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.

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 Data Protection Act 1988.

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.

3.2. Privacy

The ICT systems, infrastructure and their contents are the property of the Trust and are provided to assist the performance of your work. You should,

therefore, have no expectation of privacy in any electronic communication sent or received, whether it is of a business or personal nature.

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.

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.

Users should be aware that 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.

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

3.3. 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

3.4. Breaches of this Policy

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 related by the Trust as gross misconduct.

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

The Priory Federation 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.

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

3.5. 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.

4. Procedures

This procedure may only be amended or withdrawn by The Priory Federation of Academies Trust.

The Priory Federation of Academies Trust Acceptable Use Policy – ICT

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.