Three Spires TRUST

'Life in all its fullness'

Staff Acceptable Use Policy

Policy owner	Head of ICT & Systems
Date updated	Summer 2025
Review date	Summer 2027

Scope of the Policy

This policy applies to all members of The Three Spires Academy Trust ("the Trust") community. This includes but is not limited to every employee, Governor, Trustee, Member, worker (including any agency, casual or temporary worker), volunteer and contractor who is employed or otherwise engaged at any academy operated by the Trust and are users of any of the ICT systems at any of the Trust's academies (whether inside or outside of school hours) (each a "System User").

Technological methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures. The Trust has prepared this policy to inform you of your obligations as a System User in respect of the use of the Trust's ICT systems.

Aims

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

- The Trust ICT systems including email and internet access 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 ICT system are provided to currently employed staff or enrolled students.

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 Inappropriate use could result in access being withdrawn and an investigation to determine whether disciplinary action should follow from such use.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 individual academies central network computing account and password. Initial default passwords issued to any user should be changed immediately following notification of account set up. Use strong passwords that cannot be easily guessed. These must be kept private.
- 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. It is recommended that all staff users change system passwords at least once per 90 days, a system-initiated change will be enforced within this time frame.
- 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 2018.
- The policies set out in this document apply to all staff members and students within the Three Spires Trust. 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.
- All staff must use Two-Factor Authentication (2FA) when accessing Trust systems that support it, including Microsoft 365, MIS platforms, and cloud services. 2FA adds an essential layer of security by requiring a second form of verification—such as a mobile code or app prompt—in addition to a password. This helps protect sensitive data from unauthorised access and supports our commitment to safeguarding and data protection.

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 and its academies reserve 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 checks will be made of the ICT systems, including internet activity logs to check for inappropriate access of websites. Where such files are located, further action as is necessary will be taken to ascertain the contents and if necessary to remove them without the consent of the owner.

Reasons for monitoring include:

- Operational effectiveness and security.
- 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.

Access to staff files including emails will only be given when authorisation is obtained from the Chief Executive or other members of academy senior leadership teams. Such action will be granted in the following but not limited to 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.

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 your own 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 (for example using personal cloud storage).
- Using personal devices to store images or other personal data.

Policy Breachers

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 like 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.

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

The Trust has a legal duty to safeguard and promote the welfare of children, young people and vulnerable adults. The Trust takes its safeguarding duties and responsibilities very seriously and we consider it to be the highest 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.

Three Spires Trust IT services would suspend computer and network privileges of a user pending an investigation.

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 Three Spires Trust and its Academies.
- 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 because of investigation or formal disciplinary action.

Policy Changes

This policy may only be amended or withdrawn by the ICT Business Partner and Three Spires Trust.

Three Spires Trust Acceptable Use Policy

	Signed	Name	Date
Staff Member			

Principal			

Agreement