Staff ICT Use Policy
Dated June 2018
Review Period 3 Years
Finance and Staffing Committee
Author NF
Approved by the Trustee Board on 17 July 2018
Reviewed and updated by Author March 2021
Reviewed by IR March 2023
Reviewed by IR, SW and DH June 2024
Approved by the Trustee People Panel 0n 04 July 2024
Reviewed by DH 28 May 2025
Approved by the Trustee People Panel on 19 June 2025
Reviewed by DH 05 May 2026
Approved by the Trustee People Panel on 15 June 2026

# ACCEPTABLE USE OF THE ICT AND COMMUNICATIONS SYSTEMS FOR STAFF POLICY

## 1 Purpose and Scope

1.1 The policy is designed to:

a) help employees, trustees, governors, and other users (e.g. visitors, contractors) understand the ways in which they are and are not allowed to use The Learning Trust (TLT) and its schools' ICT and communications systems;
b) help with maintaining the security, integrity and performance of ICT systems;
c) minimise both the TLT and its schools' and users' exposure to possible legal action arising from unauthorised use of the ICT and communications systems;
d) help ensure that TLT and its schools can demonstrate effective and appropriate use of publicly-funded resources (e.g. computers, digital devices and servers); and
e) comply with the Data Protection Act.

1.2 The policy covers not only the use of the systems and facilities provided and owned by TLT but also those personal systems used for TLT or school business when working remotely from home, particularly:

a) the Internet;
b) email;
c) Instant messaging and all social media;
d) computers and servers;
e) telephones (landline and mobiles);
f) cloud environments such as Microsoft 365, Canvas and Google classrooms.

1.3 The ICT and communications systems and facilities are provided to enable employees and other users to perform their jobs effectively and efficiently. All normal use of these systems in pursuit of TLT and its schools' business within an employee's authority to act is allowed.

1.4 Staff are not permitted to install any software onto Trust/school devices. Any software installations must be implemented by the IT team.

1.5 Some limited personal use of the ICT and communications system by employees is allowed if it is not excessive, does not interfere with their normal work or the work of others, does not involve TLT and its schools in significant expense, does not expose TLT and its schools to legal action or risk bringing TLT and its schools into disrepute and does not relate to running a private business. Usage that could be deemed to be excessive may render an employee liable to disciplinary action.

1.6 All use by non-employees is subject to the same restrictions as for employees.

1.7 USB stick/pens must not be used and all files must only be saved on the Trust/school network drives or on Trust/school provided cloud storage.

1.8 Please report any security incidents, suspected breaches, unusual computer/network activity or misuse of ICT systems to your school's Network Manager or the Trust's Director of IT.

## 2 Restrictions

2.1 The following list of unacceptable uses will render an employee liable to disciplinary action. The list is indicative and not complete.

1. Transmitting any material that infringes the copyright of the owner.
2. Purchasing goods or services or entering into any contract on the Internet on behalf of TLT and its schools without the necessary authority.
3. Business advertisements or trade sales.
4. Trading, i.e. sale of any goods purchased with the sole intention of making a profit.
5. Using an unauthorised Instant Messaging service.
6. Entering personal or sensitive Trust/school data into unapproved AI systems.
7. Sending or forwarding chain emails.
8. Making your personal user id and password available for other people to use.
9. Accessing another user's data without appropriate authorisation.
10. Deliberately creating or storing information which infringes the TLT and its schools' data protection registration.
11. Using the TLT and its schools' provided phones to make personal/non-business international calls.
12. Using the TLT and its schools' provided phones to make personal/non-business-related calls to premium rate numbers.
13. Using another person's identity to appear to be someone else on the network
14. Attempting to gain unauthorised access to another user's email, files or user account.
15. Deliberately accessing, viewing, receiving, downloading, sending or storing material:

    a) with pornographic, offensive, obscene or indecent content;
    b) related to criminal skills or terrorist activities;
    c) that promote or encourage racism or intolerance;
    d) that is illegal in the UK;
    e) that is defamatory, offensive or abusive;

f) that will bring the TLT and its schools, its staff or Governors into disrepute;
g) that is known to be infected with a virus or ransomware.

**2.2 Notes**

2.2.1 Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive or defamatory email or SPAM will not be treated as a disciplinary offence.

2.2.2 Anyone accidentally accessing a pornographic or other inappropriate web page should report the matter to their line manager. No disciplinary action will be taken in such cases.

2.2.3 Anyone accidentally viewing what they believe is illegal material (e.g. child pornography) must immediately stop what they are doing, take a note of where they found the illegal material and close the software application displaying the material. They must not view the illegal material again and must take appropriate measures to ensure that others cannot view the material.

They must then immediately inform their line manager and the school's Network Manager or Trust Director of IT (email is adequate) who will decide how to proceed. It is a criminal offence to continue to view, allow others to view, or not report illegal material.

**3 Penalties**

3.1 Any activity that falls within the definition of unacceptable use will render an employee liable to disciplinary action. Serious instances, including some sufficiently serious single instances of unacceptable use may be regarded as gross misconduct and may lead to summary dismissal. For non-employees the appropriate action will be discussed with the user's management and may lead to a bar on site access.

**4 Private/Personal use**

4.1 As a concession, employees **limited and reasonable** personal use of the ICT and communications facilities is permitted provided that such use:

a) does not interfere with their (or others') work; and
b) does not incur any additional expense for TLT and its schools and/or tie up resources needed for business.
c) does not make use of the employee's job title and place of work as part of any form of coercion or inference that the Trust endorses the communication.

Wherever possible personal communication should not take place through work email

4.2 Personal use should normally be undertaken in non-working time e.g. at lunchtime or before/after normal working hours. Very limited, occasional personal use during normal working time will be tolerated - e.g. to respond briefly to an incoming personal email or

telephone call. However, significant amounts of work time spent on making personal use of the internet, email, telephone, etc is not acceptable and may lead to disciplinary action.

4.3 Before personal use (or undertaking any social media activity on personal devices), all staff should ask themselves the following questions.

a) Would my actions be considered unacceptable if viewed by a member of the public?
b) Would managers, or others in similar positions call into question the cost effectiveness of either my use of work time or my use of the ICT and communications facilities if they knew about it?
c) Will my personal use have a negative impact upon the work of my colleagues or their morale?
d) Could my personal use bring TLT and its schools into disrepute?

**Personal use should not be undertaken if the answer to any of these questions is yes.**

4.4 Responsibility for ensuring that any personal use is acceptable rests with the individual. Staff should seek guidance from their line manager if they have any doubts concerning the acceptability of their personal use. If any doubt remains, then that form of personal use should not be undertaken and guidance sought from line management.

4.5 Staff should not accept as "friends" students of TLT on any of their personal social media sites.

## 5 Monitoring

5.1 TLT and its schools employ monitoring techniques on their communications systems, including email and Internet access, to enable usage trends to be identified and to ensure that these facilities are not being misused.

5.2 Monitoring is limited, as far as practicable, to the recording and analysis of network traffic data. To this end, TLT and its schools keep logs of calls made on each telephone and of emails sent by email address and of internet sites visited by computer system address.

5.3 These logs are routinely monitored on a continuous basis to help ensure compliance with this policy. Details are recorded in a log kept by the school's Network Manager, reported to the IT Director/Headteacher and any anomalies or patterns causing concern will be reported to the HR Team. Further investigations may be necessary where there is reasonable suspicion of misuse of facilities.

5.4 Since TLT and its schools own and are liable for data held on their communications systems, they reserve the right, as part of such investigations, to inspect the contents of any emails that are sent or received, and of Internet sites accessed, for compliance with this policy. Exceptionally, where there is a defined and valid reason for doing so, the inspection of email contents may include items marked 'private' or 'personal'. Employees' email and voicemail accounts may also be accessed by management when they are absent from work to ensure official business matters can be effectively dealt with. For the avoidance of doubt, this includes files stored within all users file storage areas.

5.5 Monitoring/investigations of employees' use of the communications systems may also happen in the following circumstances:

a) to detect or prevent crime e.g. detecting unauthorised use of systems, protecting against viruses and hackers, fraud investigation;
b) as part of occasional training and quality control exercises e.g. how incoming calls are handled;
c) to assist in maintaining the security, performance, integrity and availability of the ICT systems which support the email system and provide connection to the Internet;
d) to provide evidence e.g. of a commercial transaction, to establish regulatory compliance, audit, debt recovery, dispute resolution.

5.6 Where monitoring is used, only staff trained in data protection compliance will investigate the recorded data. Confidentiality will be ensured for all investigations involving personal data, except to the extent that wider disclosure is required to follow up breaches, to comply with court orders or to facilitate criminal investigation.

5.7 In addition, the ICT team and external auditors conduct audits on the security of the Trust's computer systems. These audits include examination of a small, randomly selected set of desktop and server systems. The audit checks that these systems have correctly licensed software, do not contain inappropriate material and have not been used to access or view inappropriate material on the Internet.

5.8 Where monitoring reveals instances of suspected misuse of the communication systems e.g. where pornography or other inappropriate material is found, or where substantial time-wasting or other unacceptable/forbidden use is found, they will be investigated through the disciplinary procedures.

## 6 Personal files, documents and emails

6.1 These are not to be stored on the TLT and its schools' systems but should be transferred to another data storage medium or device.

6.2 Printing of documents should be for business use only. However, if you wish to print personal documents, please contact the Finance Team who will be able to calculate the cost of the printing and take payment.

## 7 Information Systems Privacy and Security Guidance

7.1 It is the responsibility of individual users to keep information as secure as possible. Passwords should contain at least twelve alphanumeric characters and be changed every 90 days. Users should make every effort to conceal passwords when logging on, particularly to students. Multi Factor Authentication (MFA) must be used on all accounts where available.

7.2 Users must 'lock' or 'log out' of systems fully when leaving their devices unattended. Screen locks are installed and fitted to all computers and must not be disabled.

7.3 Users should not explore areas of the Network that are not connected with their job. Access to sensitive and confidential areas will be restricted to those who need access.

7.4 Confidential documents should have a password set by the author.

7.5 Any breaches in security should be immediately reported to the Network Manager or Director of IT.

**8 Use of email to communicate with students and parents.**

8.1 If using email or sending messages around or out of the Trust computer network or Trust registered software such as Synergy, staff must observe etiquette which means that they must only use language that is not offensive or inappropriate. Liability will apply to an email just as it would to any other material. Only business communication should be conducted with students via email. Online chat outside of school approved systems leaves adults open to misinterpretation or accusation of abuse.

8.2 Careful consideration should always be given as to whether email is the most appropriate form of communication in the first instance, but especially when the information is of a sensitive nature and/or likely to upset parents/carers.

Where the information is of a personal nature and/or likely to be upsetting then a phone call or face-to-face discussion may be more appropriate.

8.3 Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. Special care should be taken in the posting of photographs, videos and information related to the Trust, Trust life, staff and students. When using Social Media staff should comply with The Learning Trust's Social Media Policy and TLT Social Media Guidelines for Staff.

8.4 Staff are reminded that anything written or sent electronically may be retained and disclosed as part of an external Subject Access Request and should therefore be written with appropriate care.

**9 Staff AUP login screen.**

(This message will be displayed at the login screen of staff Trust/school devices. Staff click 'ok' to agree to these points.

**Use of the network:**

1. You must not share your user account details with anyone or log on to a system on behalf of anyone.
2. You must not explore areas of the network where you are not permitted to.
3. Your password should be changed every 90 days and should be a complex password, at least twelve characters long as described in the ICT Policy.
4. You must not transmit or store any data that infringes copyright or data protection laws.
5. Purchasing goods, services or entering into contracts on behalf of the Trust/school without authority is not permitted.

6. You must not use the Trust/school network to trade, or to run a private business.
7. You must not try and gain access to someone else's user account.
8. You must save all files to the network (shared and home areas) or official Trust/school cloud systems to ensure they are backed up (M365 for example).
9. USB/memory sticks are not permitted to be used.
10. You must not plug devices into hardware without prior permission from the IT support team.
11. You must not attempt to connect any personal devices to the curriculum network. They can only connect to BYOD wireless.
12. You must not attempt to change any computer settings nor bypass any security settings.

**Use of the Internet and e-mail:**

1. You may use the Internet provided by the school for work related research. Personal use is restricted to limited and reasonable use as described in the ICT AUP Policy.
2. You must not use the Internet to access illegal, harmful, derogatory, racist or explicit material.
3. You must not download material that is harmful, illegal, or could bring the Trust/school into disrepute.
4. File sharing, P2P, and torrent downloads are strictly prohibited.
5. You must not stream music or films from the Internet without prior approval from the IT support team.
6. You must not use the Internet to run private businesses.
7. You must observe the rules of e-mail (netiquette).
8. Offensive Language is not permitted and emails containing offensive language will be blocked and reported.
9. You must not send unsolicited, unauthorised e-mails that could invoke the Trust/school into contract or purchase.
10. You must not use your e-mail account to sign up to websites that deliver SPAM.
11. You must use MFA on accounts when available.
12. You must not submit personal or sensitive Trust/school data into unapproved AI systems.

INTERNET AND E-MAIL USE IS MONITORED AND LOGGED BY SECURITY SYSTEMS CONSTANTLY. LOGS ARE ALSO LOOKED AT MANUALLY BY IT STAFF AND ANY MISUSE WILL BE REPORTED.

**Software:**

1. You are not permitted to install any software on any Trust/school device.
2. All software installation requests must be made to the IT support team.
3. All software must be correctly licenced. Proof of licence will be required before any installation.

**Home use:**

Where a device is portable (e.g., laptop) and is booked out to you, you may use this device at home for work related use only. This device will be monitored in the same way that it would be if it were used in school.