ACCEPTABLE USE OF THE ICT AND COMMUNICATIONS SYSTEMS FOR STAFF

1 Purpose and Scope

1.1 The policy is designed to:

a help employees and other users (e.g. visitors, contractors) understand the ways in which they are and are not allowed to use the CLT & its schools' ICT and communications systems;

b help maintain the security, integrity and performance of the ICT systems;

c minimise both the CLT & its schools' and users' exposure to possible legal action arising from unauthorised use of the ICT and communications systems; and

d help ensure that CLT & its schools' can demonstrate effective and appropriate use of publicly-funded resources.

e comply with the Data Protection Act 2018.

1.2 The policy covers use of systems and facilities provided, particularly:

a the Internet

b email

c Instant messaging and all social media

d computers and servers

e telephones (landline and mobiles) and faxes

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 CLT & its schools' business within an employee's authority to act is allowed.

1.4 Some limited personal use of the ICT and communications system by employees is allowed provided that it is not excessive, does not interfere with their normal work or the work of others, does not involve CLT & its schools' in significant expense, does not expose CLT & its schools' to legal action or risk bringing CLT & 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.

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

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.

a Transmitting any material such that this infringes the copyright of the owner.

b Purchasing goods or services or entering into any contract on the Internet on behalf of CLT & ITS SCHOOLS without the necessary authority.

c Business advertisements or trade sales.

d Trading, i.e. sale of any goods purchased with the sole intention of making a profit.

e Using an unauthorised Instant Messaging service.

f Sending or forwarding chain emails.

g Making your personal user id and password available for other people to use.

h Accessing another user's data without appropriate authorisation.

j Deliberately creating or storing information which infringes the CLT & its schools data protection registration.

k Using the CLT & its schools' -provided phones to make personal/non-business International calls (except where calls are booked via the Bursar and paid for by the user).

m Using the CLT & its schools' -provided phones to make personal/non-business related calls to premium rate numbers.

n Using another person's identity so as to appear to be someone else on the network

p Attempting to gain unauthorised access to another user's email.

q Deliberately accessing, viewing, receiving, downloading, sending or storing material:

1 with pornographic, offensive, obscene or indecent content;

2 related to criminal skills or terrorist activities;

3 that promote or encourage racism or intolerance;

4 that is illegal in the UK;

5 that is defamatory, offensive or abusive;

6 that will bring the CLT & ITS SCHOOLS, its staff or Governors into disrepute;

7 that is known to be infected with a virus.

2.2 Notes

2.2.1 Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive or defamatory email. 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 (i.e. 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 (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 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 CLT & its schools' and/or tie up resources needed for business.

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

4.3 Before undertaking personal use (or within 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, auditors 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 CLT & 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 still 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 The Learning Trust on their personal social media sites.

5 Monitoring

5.1 CLT & its school's employ monitoring techniques on its 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, CLT & its school's keep logs of calls made on each telephone and fax machine, 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 ICT Manager, reported to the Bursar and thence to the Staffing Committee annually.
Further investigations may be necessary where there is reasonable suspicion of misuse of facilities.

5.4 Since CLT & its school's owns and is liable for data held on its communications equipment and systems, it reserves 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.

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. Logged data will not be retained in accordance with the Data Protection Policy.

5.7 In addition, the ICT team and external auditors conduct audits on the security of the Trusts 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 CLT & its school's systems but should be transferred to another data storage medium or device.

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 6 alphanumeric characters and be changed every 30 days. Screen locks are installed and fitted to all computers and must not be disabled. Users should make every effort to conceal passwords when logging on particularly to students.

7.2 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.

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

7.4 Any breaches in security should be immediately reported to the Network Manager.

8 Use of email to communicate with students and parents.

(see full internal procedure to be contained within Staff Handbook and posted on the Trust's website)

8.1 If using email or sending messages around or out of the Trust computer network, 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 leaves adults open to misinterpretation or accusation of abuse.

8.2 Information likely to upset parents/guardians should not be sent by email in the first instance. All communications with Parents and students must adhere to the Communications protocols as shown within the Contact Us section on the Trust's website.

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. Particular care should be taken in the posting of photographs, videos and information related to the Trust, Trust life, staff and students.

Approved by the Trustee Board on 17 July 2018