TRUE LEARNING

PARTNERSHIP

ICT ACCEPTABLE USE POLICY	
Policy Ref Number: TTLP/53	**Reviewed by: HR Director/IT Director**
Policy Date: July 2022	**Review Date: July 2023**

APPENDICES

This document will be issued annually and each employee will be asked to confirm that they have read and understood the contents. This information is recorded digitally and held centrally.

1. INTRODUCTION

1.1 For the purposes of clarity 'Trust' refers to The TRUE Learning Partnership (TTLP) and the schools within in it.

1.2 The increasing use of Information and Communications Technology necessitates an ICT Acceptable Use Policy to ensure these systems are developed, operated, and maintained in a secure manner.

1.3 The ICT Acceptable Use Policy works alongside additional policies including:

- TTLP Safeguarding Statement and individual school Safeguarding Polices.
- TTLP Employee Code of Conduct
- TTLP GDPR Policy
- TTLP Social Media Policy

1.4 This Policy will apply to all employees who should be aware of the contents of the policy along with the importance of information security and their responsibilities for security whilst working in Trust/school premises or off site.

1.5 It is not the intention of the Policy (or resultant security controls) to be unnecessarily restrictive. The aim is to ensure there is a framework of control in place for mitigating significant risks to the Trust's information services, its employees and its reputation.

1.6 The Policy is binding on all employees who are authorised to use the Trust's IT equipment, email and the internet for Trust business and **must** be adhered to at all times.

1.7 The Trust makes no guarantee that the services provided by or through the network will be error-free or without defect. The Trust will not be responsible for any damage, including but not limited to, loss of data or interruptions of service. The Trust is not responsible for the accuracy or quality of the information obtained through or stored on the system.

2. GUIDING PRINCIPLES

2.1 The Trust is committed to safeguarding and promoting the welfare of children, young persons and vulnerable adults and we expect all employees to share this commitment.

2.2 The policy has been drawn up having regard to the following guiding principles:

- To outline the strategic framework and responsibilities for maintaining effective security over the Trust's Internet and email systems.

- To ensure appropriate levels of:

i. **Confidentiality** - ensuring information is not disclosed inappropriately.

ii. **Integrity** - safeguarding the validity, accuracy and completeness of information owned, obtained and used by the Trust.

iii. **Availability** - ensuring that information is accessible and usable when required for the business of the Trust.

iv. **Relevance** - ensuring that the Internet, email and facsimile systems are used in accordance with the business needs of the Trust.

v. **Security** - ensuring that the Trust's computer systems and equipment are used appropriately in order to avoid any damage (either willful or malicious) being caused.

vi. **Safeguarding** – to protect both employees and students.

2.3 The Policy has been drawn up in accordance with current statutory provisions relating to information systems including:

- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Data Protection Act (UK) 2018
- The Computer Misuse Act 1990
- Copyrights, Designs and Patents Act 1988

- The Obscene Publications Act 1959 and 1964
- Equality Act 2010 and now the Equality Act 2020

3. APPROPRIATE AND INAPPROPRIATE USE OF INFORMATION SYSTEMS

3.1 The Trust's IT equipment, email and internet ("Communication Resources") belong to the Trust and are to be used solely for Trust business. The Trust reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites used. However, where an employee has access to systems or equipment out of business hours and/or has obtained appropriate permission to use the equipment, and where there is no extra cost to the Trust, employees are encouraged to use these to develop their skills, knowledge and understanding.

As a general principle, computer use, email and internet access are provided to employees to support them in their work-related activities. All internet use should be appropriate to the employee's professional activity. The following list, although not intended to be definitive, sets out broad areas of use that the Trust considers to be appropriate to the employee's professional activity;

- to provide a means of business communication within the Trust and other schools, agencies and organisations.
- to view and obtain information in direct support of the Trust's business activities.
- to promote services and products provided by the Trust.
- to communicate and obtain information in support of approved personal training and development activities.
- any other use that directly supports work related functions.

It is each employee's responsibility to check with their Head Teacher to ascertain whether any proposed use, not referred to in the above paragraph, falls within the Trust's definition of appropriate use.

In addition, employees may make 'light personal use in the interests of work life balance' (i.e., banking, shopping etc. in non-working time). These activities will be allowed in moderation providing professional activity is not compromised and that the terms of this Policy are complied with.

3.2 The use of the Trust's Communication Resources to communicate Trade Union business is laid down in the Trust's Facilities Agreement: Time off for Trade Union Duties and Activities.

3.3 Any abuse or misuse of the Trust's Communication Resources by an employee may be considered a disciplinary offence.

3.4 Some examples of what could constitute a disciplinary offence under the Policy are:

- Contravention of a legal provision, e.g. The Regulation of Investigatory Powers Act 2000; The Freedom of Information Act 2000, The Data Protection Act 2018; The Computer Misuse Act 1990; The Copyrights, Designs and Patents Act 1988 and the Obscene Publications Act 1959 and 1964; See also the Trust Social Media Policy.
- use of equipment without prior consent.
- circulation of personal information, for example advertisements, offers to sell goods, etc.
- introduction of viruses.
- viewing, downloading and/or circulating illegal or offensive material from the internet.
- filming or recording of inappropriate material.
- unauthorised viewing of other people's email.
- use of email for potential offensive or defamatory purposes.
- hacking into other people's emails and systems.
- unauthorised alteration of data.
- circulation of malicious/racist/sexist/offensive material including chain letters.
- use of Trust computers/devices for personal financial gain, gambling, political purposes (beyond the remit of your role in the Trust).
- vandalism of any description. Vandalism is defined as any malicious attempt to harm or destroy hardware or data. This includes, but is not limited to, the uploading or creation of computer viruses.

3.5 Employees should be aware that any of the above could also constitute a criminal offence.

3.6 Users must be respectful of the amount and type of documents that they store in their account and on the school's ICT network. No personal music, photographs or DVD's /Video's should be stored on Trust Communication Resources. This also applies to the use of work-related mobile devices (i.e. iPads, iPhone etc.) and care should be taken in particular to ensure that material is not shared across devices inadvertently or otherwise through use of an AppleID or other platform that links devices or duplicates content. Any queries or concerns in relation to the safe storage of downloadable items for personal use should be directed to the Director of ICT and Network Operations.

4. COPYRIGHT & LICENSING

4.1 All employees are responsible for ensuring that copyright and licensing laws are not breached. If in doubt you can seek advice from your Head teacher or CEO in the first instance.

5. ETIQUETTE AND USER RESPONSIBILITIES

5.1 Employees need to be mindful that they are acting as representatives of the Trust when using Trust Communication Resources.

5.2 Whilst employees can expect the Trust to respect their privacy there are certain exceptions, in relation to the Communication Resources where employees should be aware that there is routine monitoring by the Trust (see Section 7 Monitoring).

5.3 Although each employee has a password to his/her computer, this does not guarantee privacy or security. Hackers can enter networks; information transmitted can also be captured by other internet sites.

5.4 Head Teachers, the CEO and the Chair of the Trust should ensure, through their Professional Development cycle and appraisal process, that appropriate training is made available to employees who have access to Trust Communication Resources as required.

5.5 Head Teachers, the CEO and the Chair of the Trust are responsible for ensuring employees understand their rights and responsibilities regarding the use of the Trust's Communication Resources. Head Teachers, the CEO and the Chair of the

Trust must ensure employees receive a copy of this Policy and any subsequent amendments.

5.6 Leaving a password close to a device or leaving a device on overnight may render security systems ineffective. Employees should therefore ensure that devices are switched off at the end of their working day and passwords are kept secure. Passwords should never be made available to another person.

5.7 Employees should use multifactor authentication when possible in line with the requirements from the risk protection arrangement (RPA) cover

5.8 Employees using Trust Communication Resources outside of school must always be mindful of security and opt for the highest levels of security when using the internet to protect data.

5.9 Employees who have access to laptops, and any other mobile equipment, are responsible for the safety and security of any such equipment.

5.10 Employees should be aware that an email, or accepting terms and conditions to access an IT platform, can constitute a contract. Therefore, it is the responsibility of each employee to ensure that the content of emails is correct and appropriate, whether they are sending or receiving emails or otherwise using Communication Resources.

5.11 Employees must ensure that they always include and do not deactivate or invalidate the disclaimer (at Appendix 1) from communications.

5.12 IT Programmes other than those provided by the Trust should not be loaded without prior permission. Any activity that threatens the integrity of the Trust's Communication Resources, or that attacks or corrupts other systems is forbidden. Employees must ensure they do not deactivate the virus scanners on their systems.

5.13 Employees must refer to the Director of ICT & Network Operations when using Cloud Storage for any data to ensure security.

5.14 If an employee unintentionally accesses an internet site which contains material of an offensive or undesirable nature, he/she should immediately exit the site and report the incident to his/her Head Teacher, the CEO or the Chair of the Trust as appropriate who may prevent future access to such sites by implementing

preventative measures having consulted with the Director of ICT & Network Operations.

5.15 To avoid any damage and unnecessary repair costs, employees must contact the Trust's IT Support in accordance with local procedures in the event of there being a problem with the Trust's printers and copiers, and should not attempt to fix the problem themselves

5.16 All employees are asked to reduce printing and copying volumes and use of paper where this is possible and does not compromise their work.

5.17 All employees must protect and take appropriate care of Trust ICT equipment. The Trust may consider recouping costs from departments or individuals on a case by case basis.

5.18 The use of school laptops and portable mobile devices at home is allowed, but the transferring of information that contains student or employees' details to home computers or other privately-owned IT devices in any format, including but not limited to photographs or videos, is strictly forbidden in line with our Data Protection Policy.

5.19 The use of privately-owned laptops and/or handheld mobile devices on the school network is allowed in some circumstances but the transferring of information that contains student or employee details to such equipment in any format, including but not limited to photographs or videos, is strictly forbidden in line with our Data Protection Policy.

5.20 Communication with parents/guardians and students must only be made through appropriate school communication channels i.e. school email or any other designated parental contact channel approved within your school/Trust.

5.21 Employees must not contact or communicate with parents/guardians and students or carry out any Trust business using personal social media accounts such as Facebook, Twitter, Instagram and LinkedIn.

5.22 The Trust expects the utmost integrity when employees use any social media platforms either on behalf of the Trust and its schools or personally and specific guidance is available to employees in the TTLP Social Media Policy.

5.23 Employees and students using digital cameras, video or sound recorders must ensure that they inform and explicitly ask permission of others before recording and always use such equipment in a respectful manner. All images relating to students or the Trust must immediately be transferred to the designated network drive for security. Employees must verify that parent/guardian permission has been given for the use of photographs, this permission is held for individual students in the MIS system.

5.24 Employees wishing to set up a personal device to receive school emails should ensure that the device is not accessible to anyone else (e.g., family members). It is strongly recommended that a separate application is used for school emails (e.g., Microsoft Outlook) to ensure that they are kept separate from personal mail. Appropriate security (strong passwords or biometric protection) should be used to ensure the account remains secure. Any loss or theft of a personal device that grants access to a school email account should be reported immediately to the Trust IT team.

6. UTILISATION, RETENTION AND DELETION OF FILES

6.1 Emails or texts are a form of publication. Employees as well as the Trust are potentially open to action for libel, defamation or breach of trust.

6.2 Whenever an external email is sent an employee's name, job title and email address must be included on the email. The Disclaimer, attached at Appendix 1, will automatically be included on external emails.

6.3 Employees need to be aware when composing emails or texts that messages can easily be misconstrued and therefore the message being transmitted should be accurate and relevant to the recipient. The same professional levels of language and content should be applied as for letters or other media, particularly as email and texts are often forwarded.

6.4 Forgery or attempted forgery of electronic mail is always prohibited.

6.1 Head Teachers or other designated persons will have access to emails when this is necessary, for example, where employees are absent on leave or through sickness. Emails are not a private means of communication but a record on behalf of the Trust of work-related matters. It is important to remember that an email or fax is not private. Email documents form part of the administrative records of

the Trust and the Trust has the right of access to all emails sent or received, on the same basis as any other written documentation.

6.5 If an employee receives an email or text from outside the Trust that is considered to be offensive or malicious then he/she must forward it to the Trust IT Team immediately and should not respond to it.

6.6 Employees must not open email attachments from unknown sources in case these are harmful and should seek guidance from the Trust IT Team in this event.

6.7 In order to ensure compliance with the requirements of the Trust and the contents of this Policy, monitoring software may be utilised to check on the use of email and internet services, as well as software to check the content of email messages sent and received.

These software tools will only be used for the legitimate purposes of ensuring compliance with legislation, policies and guidelines so as to protect the Trust against the risk of criminal and civil actions that may arise, as a result of the unauthorised actions of its employees, and in connection with the administration of the email and internet service itself.

Employees should be aware that email messages, or other communications could ultimately be required to be disclosed in Court.

6.8 Employees are responsible for ensuring hard copies of formal communications are made when appropriate and stored or filed in accordance with Trust requirements and where appropriate, statutory requirements. Formal documents can include emails that replace letters, confirmation, agreements, requests for information, etc. If in doubt employees should seek guidance from the Head Teacher/CEO.

6.9 Email communications and any other communication records held by or on behalf of the Trust may be subject to the Freedom of Information Act, so that anyone may be entitled to access to them through a subject access request, unless exempt from disclosure under the Act.

6.10 Employees should follow the retention schedule contained within the Trust GDPR Policy.

7. MONITORING

7.1 The Trust, when monitoring the application of this policy, will ensure it always complies with the relevant legislation and guidance, including:

- The Regulation of Investigatory Powers Act 2000
- The Freedom of Information Act 2000
- The Data Protection Act 2018
- The Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

7.2 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows business and public authorities to record or monitor communications without consent in such cases as:

- recording evidence of transactions
- ensuring compliance with regulatory or self-regulatory rules or guidance
- gaining routine access to business communications
- maintaining the effective operation of the systems
- monitoring standards of service and training, and combating crime and the unauthorised use of systems.

In line with this legislation the Trust reserves the right to monitor email communications and records without notice.

APPENDIX 1 - DISCLAIMER

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

Unless expressly stated to the contrary, any views expressed in this message are those of the individual sender and may not necessarily reflect the views of the Trust.