ACCEPTABLE USE POLICY

Tees Valley Education Trust

Version:	2.0
Ratified by:	Trust Board
Date ratified:	December 2019
Name of originator/author:	Emma Chawner in conjunction with OneIT
Circulated to:	All Trust employees, parents/carers
Review date:	January 2021
Target audience:	All Trust employees, parents/carers

TABLE OF CONTENTS

1 STATEMENT OF INTENT

Tees Valley Education Trust's Acceptable Use Policy is linked to our business objectives and provides management direction and support for our IT users. The purpose of this policy is to ensure preservation the confidentiality, integrity and availability of the information we use. This is commonly known as the C.I.A. of information security.

Confidentiality	making sure that information is only available to those who are authorised to have access to it
Integrity	making sure that the information we use is accurate and complete
Availability	making sure that information is available where it is needed, when it is needed, and in the right format

This policy covers a whole range of information security related issues and is designed to support you in your day-to-day activities, and to protect you, Tees Valley Education, our pupils and their families, Trustee's and Members from information security incidents.

If you need any advice, guidance or further explanation on the content of this policy, or any other matter relating to information security, please contact your line manager or the Trust's IT provider.

2 LEGAL FRAMEWORK

This policy will have consideration for, and be compliant with, the following legislation and statutory guidance:

- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulation 2016/679

3 DISCIPLINARY ACTION

Failure to comply with the protocols contained in this policy and other associated policies and procedures could have serious consequences. All information security incidents and actual or suspected breaches of protocols or policies will be investigated and, depending upon the seriousness of the incident or breach, the Trust could take disciplinary action up to and including dismissal.

4 PERSONAL PROPERTY AND EQUIPMENT

Personal equipment (e.g. mobile phones, USB drives) must not be attached to Trust hardware (PCs, laptops, tablets etc.). Do not store or download Trust information onto personal equipment without formal authorisation in accordance with the agreed procedure.

5 DATA PROTECTION

In order to maintain adherence to the Trust GDPR policy, users must:

- not leave documents or sensitive, personal information unattended on printers or faxes.
- secure personal or sensitive information left on printers and report the incident to their line manager or host.
- not deliberately access or attempt to access information to which you are not authorised.
- not leave mobile phones, tablets and other portable storage devices unattended.
- Ensure mobile phones, tablets and portable devices are password protected.
- ensure that memory sticks and other removable media are properly and securely stored away when not in use.

- lock their workstation or log off before leaving it unattended.
- take care to ensure that screens cannot be overlooked when working with sensitive data.
- take care to ensure that sensitive information does not remain visible when the 'join me' shadowing system is in use.

6 PHONE/VOICE CALL

Exchanging information by phone is generally efficient and effective, but can introduce the risk of information being easily available to people other than the intended recipient. Sensitive or personal information must not be left on answer machines or voicemail. When making or receiving a call, it is essential to verify the identity of the caller/recipient and before exchanging sensitive personal information and ensure that they are entitled to receive it.

Speakerphone or conference call functions must not be used without the permission of all participants and where there is a danger of being overheard.

7 FAX

The Trust no longer permits the use of fax machines and advises use of e-mail and secure platforms such as OneDrive for sharing information. Please see the Trust issued guidance on sharing secure information and receiving secure information.

8 HEALTH AND SAFETY

Users are responsible for ensuring they have undertaken an informal personalised risk assessment before using any workstation and, where risks are identified, must report this to their line manager/Trust host.
Users are advised:

- Make sure to understand the Display Screen Equipment Regulations and Guidelines (https://www.hse.gov.uk/pubns/indg36.pdf).
- If there are problems with the positioning of equipment (e.g. glare, temperature, humidity) report it to their line manager/host.
- Food and drink is not permitted around important processing equipment such as servers, printers and MFDs.

9 PORTABLE EQUIPMENT

Portable equipment is very convenient but is more vulnerable than office based equipment, the obvious risks being

- loss of equipment and any information held on it
- use of equipment in circumstances where confidential information may be overheard or viewed
- theft, either for the equipment itself or for the information it has on it
- accidental damage

For the purposes of this policy 'portable equipment' is equipment that is owned by the Trust. This includes portable computers, mobile phones, tablets etc. Before using any portable equipment, uses should ensure they know how to use it properly. Equipment left unattended must be securely stored.

Always password protect and encrypt information stored on portable equipment and make back-up copies of important information.

To avoid unauthorised access to information take care when using portable equipment in public places, meeting rooms, and other unprotected areas outside of the workplace, e.g. if logging in to Office 365 on a public computer users must ensure they log out correctly and must not use the 'Remember me' function.

Portable equipment is issued to help staff in their day-to-day work but remains the property of Tees Valley Education and staff are responsible for keeping this equipment safe and maintained.

The issue of equipment will be recorded on an asset database and the information will be used to recover the equipment from staff when it is no longer required or the staff member has left the role. It is the responsibility of the staff member to return Trust issued equipment. Returned equipment will normally be re-issued, which means any information on it will be permanently deleted. Staff are responsible for making sure that any data that required is removed from the equipment before it is returned. The Trust will also ensure its IT provider undertakes a further check to reset the device back to factory settings and no data remaining from the previous owner.

10 REMOVABLE STORAGE MEDIA

Removable storage media is any portable media that is used to store information. This includes electronic storage devices such as CDs, DVDs, laptops, cameras, mobile phones and USB memory sticks as well as printed output. It is important that removable storage is properly controlled to protect information from unauthorised disclosure, removal, loss or destruction therefore personal removable media must not be used for storing Trust owned information and sensitive or personal information must not be stored electronically on unencrypted removable media. It is Trust policy to encrypt all laptops, tablets and USB memory sticks.

All media containing important or sensitive information must be stored in a safe, secure environment and loss of any such media must be reported immediately. Removable media containing sensitive or personal information must be disposed of securely via the Trust's IT provider.

11 EMAIL

Electronic messaging, such as e-mail, plays an increasingly important role in business communications, and it is essential that messages:

- are protected from unauthorised access or modification
- are correctly addressed to ensure they reach the intended recipient
- contain appropriate content
- are sent in line with approved policies
- comply with the requirements of any laws or regulations

The Trust therefore insists that users:

- Do not create congestion by sending trivial or unnecessary messages, or by copying them to those who do not need to see them. If emails are received that are not work related and that could be construed as inappropriate the recipient should request the sender to stop sending them.
- Do not send or forward e-mail messages or attachments that are, or may be considered as harassment or bullying, defamatory, obscene, pornographic or sexually explicit, or are likely to bring the Trust, its pupils and parents/carers, Trustees and Members or colleagues into disrepute.
- Do not send e-mail messages or attachments that divulge information concerning other employee's private affairs without the consent of the employee.
- Do not send e-mail messages or attachments that contain confidential or sensitive information without formal approval, and ensure that in all cases the email is encrypted or otherwise protected in accordance with the Trust issued Guidance for Sharing Sensitive Information Securely.
- Do not send e-mail messages or attachments that are in breach of the Data Protection Act 2018 or any other legislation restricting or controlling the disclosure of information.
- Do not amend messages received.
- Do not impersonate any other person when using e-mail.

- Do not reply to SPAM emails.
- Do not use personal email accounts (e.g. Hotmail) for business purposes.
- Do not use Trust email address for signing up to non-work related newsletters, offers, subscriptions etc.

Trust e-mails are logged and may be inspected by line management at any time without notice. E-mails are formal records and may need to be disclosed as part of investigations or in litigation. As with all correspondence, e-mails must be constructed in a professional manner.

E-mail facilities are for business use only, with reasonable private use allowed in the users own time (e.g. lunchtime or official break).

12 INTERNET

The internet is a valuable source of information, if used effectively and responsibly, but by its nature can also present a range of information security threats. Accessing the internet for personal use is permitted, within the realms of this policy, in users own time (e.g. lunchtime) and during work time is limited to appropriate business.

Deliberate access or attempted access to inappropriate websites is forbidden and could lead to disciplinary action up to and including dismissal. Inappropriate sites include sites involving material of a sexually explicit or violent nature, and material that is offensive in any way. Internet use is logged and may be inspected by management at any time without notice. The Trust retains the right to restrict or remove personal access.

Where access to a blocked site or site category is required, authorisation from the CEO/EHT/HT/HoA/COO must be obtained and they will then organise this via the Trust's IT provider.

13 TEAMS

Staff must be aware that the chat conversations in Teams are recorded as formal records, and must be used for corporate communications only. Users must recognise that the messaging chat and conversation function is not private. It is the users responsibility for their chat content, and they must abide by the conditions as details in Section 11. Any staff member found to breaching these rules may be liable to disciplinary action.

14 SOCIAL NETWORKING SITES

Social networking sites such as Facebook, Twitter and Instagram are now a really popular way for people to communicate with one another outside work. It is important to bear in mind that what is posted online is in the public domain.

Staff must not:

- make disparaging or inappropriate comments about the Trust, its staff and pupils or their families, on a social networking site.
- post remarks on a social networking site that are or could be considered as harassment or bullying, defamatory, obscene, pornographic or sexually explicit, or are likely to bring the Trust, its staff, pupils or their families, into disrepute.
- use a social networking facility to conduct Trust business, unless you are authorised to do so.
- use a work email address for the purposes of social media, unless authorised to do so.
- request or accept friend requests from pupils or their families, or vulnerable adults with whom they have work related contact.

15 INAPPROPRIATE MATERIAL

Anything that is offensive, illegal or not directly related to the Trust may be considered as inappropriate. Obvious subjects considered to be offensive include, but are not limited to, pornography, racism, sexism and violence. This includes accessing Trust information that you are not authorised to. Inappropriate material can be held in many forms, not just electronically.

Sending, receiving and accessing inappropriate material could cause damage and have serious consequences for the Trust, its staff and pupils or their families and could result in

- disciplinary proceedings against individuals, resulting in sanctions up to and including dismissal
- legal liability and prosecution
- bad publicity and damage to the image of the Trust
- damage to professional relationships amongst employees
- damage to working relationships with partner organisations

Users must not send, distribute/re-distribute or deliberately access inappropriate material. If users receive inappropriate material, it must be treat as an information security incident and reported to their line manager/host immediately.

16 EMPLOYEE MONITORING

It is widely recognised that people are the most valuable resource within a business, but could also be the weakest link in any information security management system. The potential for deliberate or accidental breaches in information security is high, due to the wide range of activities undertaken by a large number of people with a wide variety of skills and abilities.

The monitoring of certain activities can detect weaknesses in information security procedures and controls, and can protect both individuals and the Trust from the impact of security breaches. Users are therefore advised that use of Trust owned IT systems is monitored and may be inspected without notice, at any time where there is a legitimate business purpose.

17 UNAUTHORISED SOFTWARE

Unauthorised software is any software which has not been authorised for use by the Trust. Unauthorised software can be one of the main causes of expensive computer crashes and introduces a number of risks including:

- breach of copyright – using unlicensed software is legally theft
- introduction of viruses which can significantly disrupt service delivery and damage Trust reputation
- shareware which may need licensing after a trial period
- conflicts with other systems or software causing failure or unreliable performance
- registry corruption which often results in the PC having to be rebuilt

Do not load or attempt to load unauthorised software onto any Trust devices. Do not download software from the internet without the approval of the Trust's IT provider.

18 SECURITY

Where the system remains unchanged, or any changes are properly managed, the system is guarded and protected by in-built security features. However, even a small change that is not properly managed can create a weakness, exposing the system and the information it holds to potential security risks. It is therefore imperative that users do not tamper with or make unauthorised changes to any system equipment and do not attempt to rectify a problem unless authorised and qualified to do so.

19 FAULT REPORTING

To ensure the efficient and effective running of information systems, and to maximise their availability, it is important that faults to systems hardware and software are reported and recorded in an accurate and timely manner. If you come across a fault with systems or equipment report it to the Trust IT providers IT Help Desk.

20 INCIDENT REPORTING

An information security incident is any event or situation that compromises or might compromise any aspect of information security. Information security incident reporting is the effective feedback of actual, suspected or potential information security incidents. If a security incident occurs it must reported to the IT helpdesk immediately so that it can be dealt with promptly. Do not attempt to investigate the incident as evidence could be compromised and the situation exacerbated. Do not talk to anyone about the incident who doesn't need to know.

21 BACK-UP AND RECOVERY

Only information that is stored on central servers is backed-up. Any information stored on workstations (PC/laptop/tablet) or on any portable devices (such as cameras) are not included in standard back-up and recovery procedures. As a general principle important information should always be stored on a centrally managed server on the secure network. If there are unusual circumstances that means information cannot be stored on a centrally managed server, users are responsible for making sure that the information is appropriately protected from loss or damage.

For advice or guidance on how to back-up information please contact the Trust IT Provider.