ICT ACCEPTABLE USE POLICY

Date approved by Directors
December 2019

TENTERDEN SCHOOLS TRUST

ICT ACCEPTABLE USE POLICY

This policy will be reviewed annually.

DATE OF POLICY: December 2019

DATE OF REVIEW: December 2020

Members of staff responsible for Policy:

- Learning Systems Team Leader
- e-Learning Administrator
- Data Protection Officer

Signed  **Chief Executive Officer**

Signed  **Chair of the Trust Board**

Summary

Aims and Scope

This policy exists to provide a framework for the use of the Tenterden Schools Trust's IT resources. It has been written to encompass all existing and new technological deployments, even though they may not be directly referenced.

All individuals that make use of the Trust's IT resources are bound by the provisions of this policy in addition to any other Trust or individual School policies.

The Trust seeks to promote a safe use of IT to support the teaching, learning, research and other public uses the Trust is involved in. In order to provide this, the legal use of our technology and facilities is required by all staff, students, contractors and any guests.

Policy review

This policy has been created by the Learning Systems Team Leader, the e-Learning Administrator and the Data Protection Officer. The Trust has a duty to provide a safe working environment, and this document aims to enforce the safe use of all IT resources for the benefit of all individuals who use it directly or indirectly.

The Trust deals with a significant amount of personal and sensitive data. As a result, the requirements for dealing with that data are more stringent than typical use.

Keeping the Trust safe

In order to provide a safe environment, the Trust is able to remotely monitor all network and device activity. The Trust retains full control over all IT equipment, including the transmission of data, the installation of applications and upgrades, and the security policies in place to protect the equipment and the users.

By using the Trust's IT infrastructure, you agree that your data may be logged and tracked for the purpose of security and stability of the wider environment. We reserve the right to disable or block any Trust-supplied equipment, or any personal device using the Trust's infrastructure, at any time.

Unacceptable Use

The Trust networks and/or any Trust-owned devices may not be used directly or indirectly for the download, creation, manipulation, transmission or storage of:

- Any offensive, obscene or indecent images, data or other material

- Any data capable of being resolved into offensive, obscene or indecent images or material
- Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
- Unsolicited “nuisance” emails
- Material which is subsequently used to facilitate harassment, bullying and/or victimisation
- Material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation
- Material with the intent to defraud, or which is likely to otherwise deceive a third party
- Material which promotes or advocates any unlawful act
- Material that infringes on the intellectual property rights or privacy rights of a third party or that is in breach of a legal duty owed to another party
- Material that brings the School into disrepute

The Trust networks and/or any Trust-owned devices must not be deliberately used by anyone for activities which have any of the following characteristics:

- Intentionally wasting staff time and/or effort
- Intentionally wasting Trust resources
- Altering data not belonging to you, without consent
- Disrupting the work of other users
- Disrupting the School network
- Denying access to the School network and any services running through it
- Pursuing commercial activities, even in support of School business, subject to a range of exceptions which can be discussed with the Business Manager

Any breach of industry good practice that is likely to: bring the Trust or any member Schools into disrepute; damage or disrupt the Trust's IT infrastructure; or any supporting infrastructure the Trust relies on (ISPs, Telephony, etc) is regarded as unacceptable use of the Trust's IT resources.

Where the Trust’s IT resources are used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the School’s network.

Users shall not, without written consent:

- Perform data-interception, password detection or similar software or practices to the Trust network or any users of the Trust network
- Seek to gain unauthorised access to restricted areas of the Trust network
- Access or attempt to access any data outside of the remit of their role within the Trust
- Perform any “hacking” activities on, against, or via the Trust’s networks or equipment

- Intentionally or recklessly introduce any form of malicious software, including but not limited to spyware, viruses or keyloggers

If any person related to the Trust believes they may have encountered evidence of a breach of any of the above, they should make this known to the appropriate authority (such as the Learning Systems Team Leader, a Technical Engineer or a DSL/e-Safety Officer).

Devices and Data

During your time at the Trust, you may be provided with a device. You will also have limited access to personal data via this device.

The Trust Technical Support team can monitor, track and disable any Trust device at any time.

Any data generated on Trust equipment belongs to the Trust. The Trust is responsible for the maintenance and security of the devices, peripherals and data, but as a representative of the Trust you are equally responsible and may be held accountable for any damage or loss through negligence.

You must keep the device, any provided peripherals and any stored data safe and secure at all times. You are fully responsible for the device and the data, and will enforce this by:

- Not leaving the device unattended whilst it is in use
- Keeping any mobile device securely locked away and out of sight of others when you are not in attendance
- Not removing the device from any supplied case - doing so will void the insurance and you will be accountable for the cost of any repairs
- Not attempt to repair, or have repaired by any individual or organisation except for Trust Technical Support, any Trust device
- Not recording any account details, whether physically or electronically
- Not sharing any account details with anyone, including other members of the Trust
- Not installing or attempting to install any applications - any additional functionality must be passed to the Trust's Technical Support team for investigation

All users should use a secure, hard to guess password. If you have access to any personal data, you must use a unique password for every account you hold within the Trust. At a minimum, you must use a password that is at least 8 characters long and contains characters from three of the following four categories:

- Upper case character
- Lower case character
- Number
- Symbol

There may be additional complexity requirements for different types of account, which will be signposted within the software or on the device itself.

You will not be forced to change your password regularly however if you suspect that your password is known by another individual you must change the affected password(s) immediately.

All users with access to personal data relating to students, parents or staff must keep the data in accordance with Data Protection legislation including the GDPR. This means that:

- All personal data must be obtained and processed fairly and lawfully, kept only for specified purposes, held no longer than is necessary and kept safely and securely with appropriate measures in place, whether used in the workplace, hosted online or accessed remotely
- Any data being removed from the school site (such as via laptops/chromebooks, email, cloud storage or on memory sticks or CDs) will be suitably protected. This may include data being encrypted by a method approved by the school
- Any images or videos of pupils will only be used in accordance with the consents received from the pupils and/or parents

If you are accessing Trust data such as email on a personal device, this device must:

- Have an access or unlock password that abides by the Trust's password requirements
- Not be used by anyone else
- Be kept up to date

You must not download or otherwise extract any data onto or via any personal device, nor can you upload or transmit any Trust data onto any non-Trust device without explicit consent.

In the event of loss, theft, damage or neglect of a device or data, or a device that contains Trust data (such as a mobile phone that you have used to check email on), or you suspect that someone has access to any of your accounts, a full report should be made to the Trust's Technical Support team immediately. In the event of the theft of Trust equipment or data whilst in your care outside of School, you must inform the police and record a Crime Reference Number and any contact details. Any further relevant information as a result of a police investigation should also be recorded and made available to the Trust. Upon your return to work, a Theft Insurance Claim Form may need to be completed. If so, it must be done as soon as possible.

New Technological Deployments and Data Protection Impact Assessments

New technology is introduced to the Trust regularly. If you have found a product or service which may be beneficial to the Trust or an individual School, or a department within the Trust,

you must first complete an initial enquiry form. This will be used to determine whether a partial or a full DPIA is required. No additional technological solutions will be considered until the DPIA has been completed sufficiently. If the Data Protection Officer and the School or Trust agrees to the proposal, a Purchase Order should be completed and handed to each of the following individuals:

- Head of Department
- Network Manager
- Data Protection Officer (if the product makes use of Personal Data)

Consequences of a Breach

In the event of a breach of this ICT Acceptable Use Policy, the Trust may:

- Restrict or terminate a user's right to use the Trust network and/or equipment
- Withdraw or remove any material uploaded or produced by that user that contravenes this policy
- Disclose information to law enforcement agencies and take any legal action against a user where appropriate, including but not limited to claiming all costs, fees and disbursements (including legal fees)

Where the user is also a member of staff of the Trust community, the Trust may take additional action, such as disciplinary or otherwise, as it deems appropriate and in accordance with the Disciplinary Policy.