IT Security & Acceptable Use Policy

Document 7

T.E.A.M Education Trust

Approved by:	**Date:** 22 June 2020
Last reviewed on:	30 June 2020
Next review due by:	Annual Review by Trustees
List of Associated Policies:	Data Protection Policy & Appendices Privacy Notice – Pupil Privacy Notice - Workforce Record Retention & Deletion Policy Social Media Policy Bring your own device Procedure (BYOD) IT Security & Acceptable Use Policy Off Site Working Procedure CCTV Procedure Data Protection (DP) Framework Privacy Policy - Trust Workforce & Governance

CONTENTS

1 Introduction

The school's IT (Information Technology) resources are essential to the effective delivery of education and other activities, but they also present risks to privacy and data protection. We are committed to using IT resources in a way that meets our data protection legal requirements and upholds confidentiality and peoples' privacy rights.

This policy supports our Data Protection Policy, and explains how we use IT in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018), and other relevant legislation outlined in our Framework and best practice.

2 Scope and Responsibilities

This policy applies to all use of IT hardware, software, devices, networks and communications by anyone who has access to any of the school's IT resources, or to non-school owned IT resources, for anything that may impact on the school or members of the school community.

All staff are responsible for reading, understanding and complying with this procedure if they have access to IT. All leaders are responsible for supervising and supporting their team to read, understand and comply with this procedure if they have access to IT.

Our Data Protection Officer (DPO) provides assistance and further guidance on the use of IT in line with DP legislation.

3 IT Acceptable Use Standards

All staff must:

- Protect school IT resources by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
- Protect pupils from harmful or inappropriate material accessible via the Internet or transportable on computer media.
- Protect the confidentiality of individuals and of school matters, including complying with the Data Protection Policy and supporting documents, and not sharing sensitive or private information without authorisation, either intentionally or unintentionally.

4 Principles of Use

For the purpose of this policy, the use of the internet will include associated internet enabled technologies such as video messaging or conferencing applications.

- Internet and email use is integral to the effective delivery of services provided by the School. Nothing in this policy should be read as restricting the proper use of email, Internet or associated technologies for School purposes.

- Limited personal use of the School's Internet is permitted subject to these principles and guidance notes.
    - Personal use of the Internet is only permitted in your own time (e.g. before or after work and during your lunchtime) and limited to browser based activities.
    - Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of the School's email, Internet and associated systems may result in disciplinary action.
- Email: Employees are not allowed use of the School's email system for personal communication.
- If you feel you may have accidentally breached this policy, you should contact your line manager immediately, or, in their absence, a more senior manager who will record this information. See Unacceptable Use – Section 5.
- The School maintains logs of all internet, video messaging or conferencing applications, instant messaging (IM) and email use and monitors the service constantly.
- The School has in place a process to block categories of internet sites and individual sites if it is deemed appropriate.
- This policy applies to all information technology and communications equipment provided by the School which can access the Internet or send/receive email (e.g. PC's, laptops, PDA's, tablets, mobile phones with Internet access etc.).
- Any personal information sent via email, the Internet and associated services such as video messaging or conferencing applications, is covered by the Data Protection Act 2018. All staff are required to handle personal information in accordance with the Data Protection Act and the GDPR.
- Emails, including conversations recorded using facilities such as Video messaging or conferencing applications, are covered by the Freedom of Information (FOI) Act and may be disclosed as part of an FOI request for information, or as part of any legal proceedings. Always exercise the same caution on email content as you would in more formal correspondence.
- Consent must be obtained for any recordings of conversations resulting from the use of facilities such as video messaging or conferencing applications.
- All employees are required to maintain the good reputation of the School when using Internet and email. Use of email and the Internet which brings the School into disrepute may result in disciplinary action.
- The School reserves the right to withdraw Internet access or email use or any access to the School's computer or communications network, if the user has been found to be in breach of these guidelines.
- The content of incoming email is automatically scanned to detect computer viruses, however, the actual text of the email is not viewed as part of this process.

- Desktop and document sharing capabilities of facilities such as Video messaging or conferencing applications, must only be used with colleagues of the School for collaboration purposes. If you allow changes to be made to these documents during a desktop sharing session as the 'sharer' of the document, it is your responsibility to ensure that the documentation is used correctly and saved appropriately.

5 Email

5.1 Personal Use

Personal use of derbyshire.sch.uk/stubbinwood.teameducation.org email or any other email system provided for use as a School employee, is not permitted at any time.

If a genuine emergency arises you should inform your line manager at the earliest opportunity that you have responded to the email and they will make a note of it. You should inform the sender that personal use of the School's email system is not permitted and an alternate method of communication will need to be considered.

It is inappropriate to use your school email address for personal use as it may give the impression that any business is on behalf of the School.

5.2 General guidance

Email is an extremely efficient means of communication but always ask yourself whether a quick internal telephone call would be more effective than sending an email message.

Emails should only be kept in your inbox for a limited time as recommended in the retention schedule. Any emails that you need to keep beyond this period should be moved to appropriate file storage.

You must only use School provided email systems to send and receive School information.

You must not use the email system in any way that is insulting or offensive. Any authorised personal data sent externally by email e.g. to solicitors, Inland Revenue etc. must be sent in compliance with the Secure Email Policy.

You must not use anonymous mailing services to conceal your identity when mailing through the Internet, or falsify (spoof) emails to make them appear as if they have been sent from someone else.

All emails are automatically tagged with the classification 'controlled'. You should consider whether you need to change the classification to 'public' or 'restricted'.

If you receive an email that is inappropriate or abusive, you must report it to your line manager immediately, who will take the appropriate action. If the sender is known to you, inform them that they should cease sending the material.

The content of all emails may be viewed by the School in certain circumstances; for example, in connection with disciplinary investigations or Audit reviews.

When emailing multiple recipients, the 'TO' box should be addressed to an address within the organisation (eg info@teameducation.org) it is essential that the BCC option is used to add email addresses so access to email addresses is not inadvertently disclosed.

5.3 Email Disclaimer

A disclaimer is automatically attached to all emails sent from the School informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of the School.

5.4 Access to email

Where an employee is absent, the employee's line manager may authorise access to a School email account to obtain messages that are work-related. The manager will inform the employee of this access on the employee's return.

6 Instant Messaging (IM)

Instant Messaging is a form of real time communication between two or more people based on typed text. The text is conveyed via devices connected over the Internet or an internal network/intranet. Messages are retained in your conversation history in your email folder list or are saved as emails in your inbox if the recipient does not respond immediately.

You must only use School provided internet messaging (IM) services. IM should not be used as a substitute for email. IM should be used only for questions or announcements that are short and need to be communicated immediately.

Private use of instant messaging for any purpose is not permitted.

7 Internet Use

7.1 Personal Use

Personal use of the Internet is not allowed during working hours. You can use the Internet before you start work, during your lunchtime, or after work. You must not, in any way, distract others from their work.

You must not use the School's Internet or email systems for trading or personal business purposes.

You are advised not to conduct online payments. This is due to the information being stored locally on your computer, which potentially could be compromised, putting the user at financial risk. If you use the Internet to buy goods or services, the School will not accept liability for default of payment or for security of any personal information you provide. Goods must not be delivered to a School address.

All Internet sessions should be terminated as soon as they are concluded.

More information on the use of other social media can be found in the School's Social Media Policy.

7.2 Filtering Content

Many Internet sites that contain unacceptable content are blocked automatically by the School's systems. However, it is not possible to block all "unacceptable" sites electronically in all circumstances.

7.3 Downloading Material

Downloading of video, music files, games, software files and other computer programs is not permitted. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

Online Mapping Software should not be used unless for specific work purposes as it is resource intensive and involves downloading an application to your computer.

Streaming media, such as radio or tv programmes, for non-work related purposes is not permitted.

If you are in doubt about software use or installation, seek guidance from the Data Protection Officer.

7.4 Accidental Access to Inappropriate Material

You may receive an email or mistakenly visit an Internet site that contains unacceptable material. If this occurs, you must inform your line manager or a more senior manager immediately.

Your manager will ask you for details relating to the incident and you will be asked how the event occurred. This information may be required later for management and audit purposes.

7.5 Copyright

You may be in violation of copyright laws if you simply cut and paste material from one source to another. Most sites contain a copyright notice detailing how material may be used. If you are in any doubt about downloading and using material for official purposes, you should seek legal advice.

7.6 Unacceptable Use

You must not deliberately view, copy, create, download, save, print or distribute any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence

- promotes any form of criminal activity
- contains unwelcome propositions
- involves gambling, multi-player games or soliciting for personal gain or profit
- contains images, cartoons or jokes that may cause offence
- appears to be a chain letter
- brings the School into disrepute or exposes it to legal action

This list is not exhaustive and the School may define other areas of unacceptable use.

8 Monitoring

Monitoring of email and Instant Messages

The School's email system automatically records details of all email sent both internally and externally. The automatic system highlights the use of certain prohibited words and any potential infringement will be referred to Senior Leaders as part of routine reviews.

The School may read and inspect individual emails and attachments for specific business purposes or during disciplinary investigations including:

- Establishing the content of transactions,
- Ensuring employees are complying both with the law and with the School's email policy, and
- Checking email when employees are on leave, absent or for other supervisory purposes.

The School routinely produces monitoring information, which summarises email usage and may lead to further enquiries being undertaken.

Monitoring Internet Access

The School records the details of all Internet traffic. This is to protect the School and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

The logs record:

- the network identifier (username) of the user,
- address of the Internet site being accessed,
- where access was attempted and blocked by the system,
- the Web page visited and its content,
- the name of any file accessed and/or downloaded,
- the identity of the computer on the network and the date and time.

Any excessive or inappropriate use may result in disciplinary action being taken.

All monitoring information will be kept for six months.

9 Passwords

Access to applications and information is controlled to protect you and our organisation. It's important that the passwords you use are strong and safe enough to keep our data secure.

9.1 Choosing a secure password

When choosing your passwords:

- keep all account log in and system passwords private
- never write down your passwords or share them with anyone
- use a strong password - at least 12 characters with upper and lower case letters, numbers and special characters like asterisks or currency symbols

Don't choose a password based on any personal data such as your name, age, or your address. Avoid using words (English or otherwise) as well as any proper names, names of television shows, keyboard sequence or anything else that can be easily guessed or identified.

Putting punctuation marks or other symbols at the beginning or end of words is not advised either.

For security, passwords should be a minimum of 12 characters long and contain a mixture of digits, letters and non-alphanumeric characters.

9.2 Methods for choosing passwords

While there are no perfect methods of selecting a password, we have identified a few tips and tricks to try and help.

Make up a sentence you can easily remember.

Some examples:

- •My uncle Joe walks his 3 dogs in the park every morning.
- •I like to eat Ben & Jerry's ice cream for dinner

Now, take the first letter of each word in the sentence and include the punctuation. You can add extra punctuation in if you like, or turn numbers into digits for variety and add special characters. The sentences would become:

- •%MuJwh3ditpem
- •$IlteB&Jic4d

9.3 Don't write your password down

You should avoid writing down your password or giving it to others. You should especially avoid writing it down and leaving it in a non-secured place such as on a post-it on your monitor or a piece of paper in your desk. If you absolutely must write something down, we suggest doing the following:

- don't write down the entire password, but rather a hint that would allow you (but nobody else) to reconstruct it
- keep whatever is written down in your wallet or other place that only you have access to and where you would immediately notice if it was missing or someone else gained access to it

10 IT equipment issued to staff

The laptop (or other equipment) remains the property of the School and is provided to users on a loaned basis. The laptop must not be used by anyone other than the authorised user to whom it has been allocated.

The property identification tag attached to each laptop should not be removed for any reason.

School laptops have a predetermined list of software installed on the hard drive. No addition or deletion of any software or hardware is permitted without the express permission of the Principal or School IT Technician. This includes the setting up of web-based accounts. Software and web based accounts that require personal data may be subject to a Data Protection Impact Assessment and so must not be installed or set up until this has been carried out. To ensure that security patches and virus definitions are up to date staff should connect the laptop to the School network on a regular basis.

All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, devices should never be left in a vehicle overnight or other unsecured, vulnerable situation. See the Offsite Working Procedure for more guidance.

Any loss or damage to School IT equipment should be immediately reported to the Principal.

When a contract of employment at the School ends, the member of staff must return all computer equipment and software to the School IT Technician in full working condition. The user account and all personal work stored on the laptop will then be securely deleted.

If software/hardware problems arise, a laptop may need to be restored to its original settings. Work files may be lost during the restore process, therefore it is the responsibility of all users to ensure that backups of all files are regularly made to an external device such as the School's networked server or encrypted mobile device.

Where there is evidence that the equipment has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any school equipment whilst on loan.

Staff should make careful, considerate use of the school's IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.

11 Clear Screen

It is essential, in order to protect both yourself and the sensitive information you have access to, that you lock your screen (laptop / PC) whenever it is unattended – even if only for a moment.

In classrooms, screens must be set to EXTEND to the Interactive whiteboard rather than DUPLICATE.

12 Use of other School IT Equipment

Users who borrow equipment from the school must sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.

Any loss or damage to equipment on loan should be immediately reported to the Principal or School IT Technician in the first instance and any theft or criminal damage should be reported to the Police.

To prevent data loss and ensure consistent application of School policies no personally owned equipment should be attached to the School's network without the permission of the Principal. All mobile devices must be encrypted or password protected wherever technology allows.

13 Software

Users should use software in accordance with applicable licence agreements. It is a criminal offence to copy software or any supporting documentation protected by copyright.

The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the school.

14 Network Access and Data Security

Users must only access information held on the School's computer systems if authorised to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information held on the school network or IT equipment be disclosed to unauthorised persons.

If you accidentally access information which you are not entitled to view report this immediately to the Principal as a data breach.

Staff using computers in classrooms must ensure that confidential or sensitive data is not accessible to pupils or anyone else by logging off or locking the computer when away from the computer. In other areas, computers must not be left logged on when left unattended.

14.1 Encryption

Sensitive or confidential information should be accessed via the network and should not be permanently stored on laptops or other portable devices e.g. memory sticks. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using an encrypted memory stick provided by the school.

15 Disposal of Computing Resources

Computing resources will be disposed of in line with WEEE regulations, The Hazardous Waste Act, The Environmental Protection Act 1990, The Environment 1995 and The Data Protection Act 2018

Governor approval will be sought before Computing resources are disposed.

If a third party contractor is used, suppliers will be suitably accredited and disposal certification will be obtained.
Following Governor approval, all equipment which contains sensitive files will have their hard disk drives wiped. (This may be done on site or via an approved contractor)

Finally, the school's inventory will be updated.

16 Backing Up Procedures

16.1 Administration System:

The School ensures that systematic back up of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.

Back up copies will be securely stored against theft, corruption or physical damage, so that in the event of a major incident a back up copy is available.

16.2 Curriculum System:

Work is backed up weekly.

Removable media are encrypted and stored securely away from the server .

17 Disaster Recovery Procedures

In the case of a disaster staff should refer to the Critical Incident Plan and ensure the following are readily available:

- An up to date list of contacts to assist in the recovery process, e.g. Principal /IT provider.
- A list of procedures and actions required by key individuals in the event of a critical incident.

The contingency plan must take into account any staff changes and be easily accessed and understood.

The school should ensure all items are appropriately insured.

18 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to School assets, or an event which is in breach of the School's security procedures and policies.

All School employees, supply staff, governors, contractors, and volunteers have a responsibility to report security incidents and breaches of this policy as quickly as possible through the School's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the School

The School will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. Suspected misuse of the School's computer systems by a member of staff will be considered by the Principal. In the case of an individual then the matter may be dealt with under the disciplinary process.