ICT Security Acceptable Use Policy

If you require this document in an alternative format please contact office@tssmat.staffs.sch.uk or 01543 472245

Last review date:		July 2021		
Next Review date:		July 2024		
Review Cycle:		3 Years		
Statutory Policy:		No		
Publication:		Website. G/Policies		
Owner		J Wynn		
Date	**Version**	**Reason for change**	**Overview of changes made**	**Source**
27.01.2021	0.1	Update to internal processes	Name & Logo update. Additional info on cyber security measures J Bowman	SCC
19.05.21	0.2	SLT review of changes	No changes made. SLT	
15.06.21	0.3	Board lead review	Minor changes. P Halifax	
09.07.21	1.0	Scheduled Board review	Ratified	

Acceptable Use Policy

Purpose

This policy is intended to provide a framework for such use of the Trust's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

Scope of Policy

For the purpose of this policy, any electronic, mobile, computing device (for example laptop, netbook, tablet, and mobile phone) will be referred to as a 'device'. Staff, employees, volunteers, Directors, Members, third parties, pupils, contractors, and any other external party may be referred to as a 'user' for the purposes of this policy.

Any reference to 'the employer' or 'the Trust' refers to The Staffordshire Schools Multi Academy Trust. Any reference to the 'network' includes software and subscription services such as Office 365, Evidence Me, Class Dojo and Google. The 'appropriate level of authority' should be determined according to the Trust's decision making structure. This policy applies to any users who have access to the network or software/services subscriptions, but does not form part of any contract and can be varied from time to time, in order to comply with legal and policy requirements and in consultation with the appropriate bodies.

Throughout this policy any reference to; wireless, WiFi, network, broadband, internet access, and infrastructure (switches, cabling, routers, wireless access points) will be referred to as 'connectivity services'.

Users of the Trust's devices are bound by this policy. The Trust seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching and innovation to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to users within the Trust.

Acceptable Use

All users, devices and connectivity services

1. When logging on to the network, users must always use their own username and password.
2. Any user who identifies a security problem on the Trust's network must notify the Headteacher immediately.
3. Users must follow the Trust password guidance (Appendix 4) Any user who suspects that their password has been compromised, accidentally or otherwise, should change their password without delay and report this potential security breach to the Headteacher and the Data Protection Officer.
4. Users must not use devices connected to the network to gain unauthorised access (hacking) to any computer network.
5. Users must not attempt to spread computer viruses or conduct any malicious act through the use of the network.
6. Users must understand that the information they hold on the network is not private and can be inspected, in compliance with applicable English law, at any time by a member of the SLT, the Board of Directors, or Members. This includes documents, emails, and web browser history.

7. Users must understand the network employs several monitoring technologies to record access to the internet, keystrokes and catalogue open windows for the purposes of safeguarding children and young people. Reports are pulled from a monitoring system and reviewed by administration staff daily. The system is set to pick up keywords relating to safeguarding and criminal activity. Any concerns raised by the reports will be directed to the Headteacher or CEO by the administration staff, and may be dealt with under the Disciplinary Policy, depending on the nature of the report.
8. Users must not store personal documents/pictures/music on the Trust's network.
9. Before leaving a device/network, users must always log off or lock their device and check this procedure is completed.
10. Users must not attempt to gain access to any trust device to create local accounts (administrative or otherwise) to disable or workaround any safeguards or security controls.
11. It is strictly forbidden for unauthorised users to attempt to set up new share drives or folders across the network.
12. Only software that has been provided by TSSMAT may be run on the computers unless prior consent from the Headteacher is obtained. Users are not permitted to import or download applications or games onto shared machines. All software purchase must go through the usual purchasing processes, and all software will be examined by the IT Provider prior to installation.
13. Pupils will ensure that they have permission to use the original work of others.
14. Where work is protected by copyright, users will not download or distribute copies (including music and videos).
15. Users must be aware of and adhere to the NCSC 10 Steps to Cyber Security, a copy of which can be found here https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

Employees/Staff

1. Staff are reminded that they have duty of care with regards to Child Protection, Safeguarding and Radicalisation, and should refer to the appropriate policy or DSL/DDSL.
2. Staff must not disclose to a third party the personal or sensitive data details of another member of staff, pupil or a pupil's family. When sending emails, staff should ensure the anonymity of addresses by making use of the BCC (blind carbon copy) functionality when addressing bulk emails.
3. Staff must ensure that they do not retain copies of personal details, including photographs of another member of staff, pupil or a pupil's family on their personal devices. Paper copies of lists and/or other pupil data should not be taken home.
4. Staff must ensure that the memory of iPads and cameras are wiped after use, and that memory sticks are wiped once images are uploaded, and stored securely.
5. Staff should ensure devices connected to trust accounts are kept secure whilst in and out of school and report any loss to the Headteacher and Data Protection Officer immediately.
6. Staff must not store school/trust material on cloud folders, unless the subscription for those services is provided by the Trust, or on external hard drives if they are not encrypted.
7. Staff should not use USB drives as storage unless encrypted, and with the prior permission of the Headteacher. These should be stored securely. All non encrypted USB drives must be from an

approved source, and have been agreed by a member of SLT prior to being used on a Trust device.

8. Staff should not use personal devices to store Trust data under any circumstances.
9. Staff must ensure they use the correct access to Trust networks when working outside a Trust school. These are remote desktops or VPN's.
10. Staff must not disclose personal or sensitive data to third parties, including app developers, without written authorisation from the Headteacher.

11. Users must be aware of and adhere to the NCSC 10 Steps to Cyber Security, a copy of which can be found here https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

Devices

Some users are provided with a dedicated device for the betterment of their teaching and learning and/or administrative duties. These devices will be fully supported and maintained by the Trust's IT Technician. By accepting the provision of a laptop/mobile device, users agree to and sign the appropriate TSSMAT document detailing our expectations. See Appendix 2 for the appropriate agreement.

Personal Devices

1. When users are connected to the TSSMAT Wireless network you are bound by all rules in this Acceptable Use Policy.
2. Users that carry a personal device on Trust premises MUST ensure that the Mobile AP or portable hotspot access point functionality is turned off.
3. Mobile devices bought on to Trust premises by any user are their own responsibility and liability. Users are strongly advised to take out adequate insurance cover as you are not covered by any Trust insurance policy.

Email & Connectivity Services

Whilst the Trust's connectivity services exist principally for enhancing the educational purposes of the Trust, staff may make personal use of Trust devices and services in their own time provided this does not detrimentally affect the Trust's primary function. Users should also be aware that all internet usage is logged.

1. Users must not breach another person's copyright in any material.
2. Users must not attempt to access inappropriate websites using the Trust's services and should be aware that all activity is monitored.
3. Users must not upload or download any unauthorised software or attempt to run that software. In particular bypassing safeguarding or security protections.
4. Users must not engage in activities that are prohibited under English Law. Thus the transmission or creation of inappropriate material, material subject to copyright or protected by trade secrets is forbidden.
5. Your email address is the property of the Trust.
6. Users must not send electronic communications which are impolite, indecent, abusive, racist or in any way intended to make the recipient feel uncomfortable.

7. Users must not make inappropriate use of the email system and address book, such as sending bulk emails, chain emails or for personal marketing purposes.
8. Staff should not use a personal email address to contact pupils or parents.
9. Trust email accounts should only be used for purposes relating to Trust matters.

Enforcement

Any breach of this policy or agreement may result in disciplinary action being taken by the Trust.

Appendix 1 – Acceptable Use Policy Agreement

Term & Conditions

In signing this document, you accept that you are solely responsible for your actions, or the actions of others, undertaken whilst using your user account or device. Your responsibility is to use the Trust's network acceptably and appropriately in accordance with the acceptable use policy. The network (its devices and connectivity services) are for the purpose of Trust related activities and it should be used with due consideration for the rest of the community who share in its use.

The Trust takes no responsibility for any personal devices bought on to the premises.

Acceptance

I accept the above policy:

Name: _____

Username (i.e 12345Smith): _____

I have familiarised myself with this document. I understand my responsibility as a user and the consequences of misuse.

Signature: _____

Date: _____

Parent/Guardian – Acceptance (Pupils Only)

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and having understood its contents grant permission for the child in my care to use and access the Trust's network.

I understand that network access is provided for educational purposes only. I also understand that every reasonable precaution has been taken by the Trust to provide a safe, secure environment but the Trust cannot be held responsible if a pupils' action is in breach of the this AUP. You have a joint responsibility to help educate your child on how to stay safe online.

Parents/Guardian of pupils are responsible for wilful or negligent damage caused by their child to any device owned by the Trust.

Name of child _____

Name of Parent/Guardian: _____

Parent/Guardian Signature: _____

Date: _____

Acceptable Use Policy

Appendix 2 - WiFi Registration (Staff & Pupils)

Agreement

The Trust is responsible for the implementation of this policy.

This document can only be actioned once the appropriate "Acceptable Use Policy" has been signed and returned.

This agreement allows additional access to the Trust's wireless network using personal devices and is an addition to the Trust's IT Security and Acceptable Use Policies.

How can I use the Wireless Network?

Step 1: Obtaining permission to connect

In order to access the wireless network you must have permission from the Headteacher, and have signed this training. Once you have read this document, please sign and date it at the bottom of the last page. Bring this signed document to the relevant school office. Once received your request will be processed within 1 working day.

Step 2: Prepare your computer

Before you bring your personal device on to Trust premises or while you are waiting for your request to be processed, please complete the following steps:

- Patch/Update your devices e.g. Windows Update or Software Update
- Install Antivirus software and ensure it is updated and fully functional.
- Remove any illegal or unlicensed software.
- Remove any inappropriate applications eg Peer-to-peer file sharing programs.

Failure to maintain a virus/malware free/ up to date operating system (patched within 1 month) device will result in immediate disconnection from the school's network without notice.

Step 3: Connecting to the network

Once you have received confirmation (via email) confirming access to the Trust's wireless network you can join ***your personally owned*** devices to the wireless network as detailed in your confirmation.
Please be aware the wireless networks are only available in specific locations, during certain hours and can be withdrawn at any time without notice.

Wireless Access Policies & Procedures

The Trust provides free wireless access to both current staff and current pupils in designated areas. The wireless network is provided ***as is*** and the Trust does not guarantee compatibility or up-time. By using the Trust's wireless network you agree to comply with this and all other policies governing the use of ICT.

- **You agree not to share your username and password with any other user for any reason.** Users found in breach of this rule will have their **WiFi access removed permanently**.
- The Trust does not provide ***any*** technical support for staff or pupils using personal devices on the wireless network apart from assisting in connecting to the wireless network itself.
- The Trust does not guarantee all devices will be compatible or the quality of the service.
- Users may not connect their personal devices to the wired network.
- The Trust may discontinue this service at any time without warning.
- I understand that the Trust will monitor my use whilst connected.

Finally the Trust accepts no responsibility for any files accessed and/or downloaded, software downloaded and/or installed, e-mail opened, or sites accessed while using the wireless network. Any damage done to the device from viruses, identity theft, theft, loss, damage, malware, plug-ins or other internet-associated programs is the sole responsibility of the user.

Unacceptable Behaviour

Users are reminded they are bound by the terms and conditions set out in the Trust's Acceptable Use Policies. The main points of the Trust's Acceptable Use Policies can be summarised in the key sentences below. Users are **NOT permitted** to undertake any of the following actions:

1. Logging on to the network with another user's account
2. Using computers to send offensive or harassing material to others, either internal or external to the trust.
3. Altering the settings of the computers or making other changes which render them unusable by others
4. Tampering physically with Trust equipment
5. Attempting to access unauthorised areas of the network
6. Accessing inappropriate web sites or trying to circumvent the safeguarding and security controls. This includes the use of proxy servers or VPNs for this purpose.
7. Attempting to spread viruses via the network
8. Using school computers for any form of illegal activity, including software and music piracy.

Breach of the acceptable use policy may result in disciplinary action being taken.

Violations/breaches

All violations or breaches of this agreement will be dealt with in accordance with the Trust's Acceptable Use, or Disciplinary Policy. The Trust may delegate this responsibility to Local Governing Bodies or school leaders. If suspected illegal activity has taken place the relevant authorities (e.g. Police) will be contacted.

Acceptable Use Policy
WiFi Registration

When bringing a personal device on to Trust premises you are fully bound by the terms of the Trust's **Acceptable Use Policies** and the use of such a device is entirely and solely at your own risk.

In order to use a personal device within the Trust, the Trust must have **on record**, a signed copy of the **Acceptable Use Policy**.

Access to the Trust's Wireless Network is a privilege, not a right, and this privilege may be withdrawn at any time at the sole discretion of the Trust without notice.

Name: _____

Email Address: _____

Signature _____

Date: _____

Please bring this completed document to the relevant school office.

Appendix 3 – Trust Issued Devices (Staff)

Acceptable Use Policy
Trust Issued Devices (Staff)

Context

Being able to use a device for, and that is provided by the Trust is a privilege and not an automatic right for staff within the Trust. The Trust must balance the need for educational freedom that a device can bring alongside the requirements set out in English law and by our own internal policies in order to deliver a compliant device that has the flexibility required for 21st Century teaching.

This policy aims to provide users with an overview of the process, what you can expect from the Trust and what access you will have to the device.

The Device

The Trust procures devices every year for use by staff within the Trust on a budget-dependent rolling programme. The device specification is driven by a need for the device to last a minimum of 4 years before it will be eligible for replacement.

Each batch of devices is supplied "as is" and no modifications can be made to the device prior to its delivery. If a member of staff wishes to customise the device after delivery they must do so themselves, whilst adhering to this policy.

Each device will have a predefined warranty attached to it, purchased by the Trust. Any issues with the device must be reported to the Headteacher immediately in order to take advantage of the warranty.

Access to the device

The Trust will ensure the device meets a standard baseline ensuring staff can use the device for its intended purpose. All devices will be "managed" (remotely accessible by the Trust) in order to deliver software updates, setting changes, enforce encryption and distribute core software.

As the recipient of a Trust device you will be permitted (in additional to the normal restrictions imposed on Trust devices) to:

- Connect to and configure Wi-Fi networks
- Install and configure printers

If additional permissions are required these will be granted at the discretion of the Trust on an ad-hoc basis.

Our expectations

To increase the longevity of any device it is important to follow these simple guidelines including but not limited to:

- When travelling the device must not be “on display”. For example when travelling by car the device ***must be*** stored in the boot and out of sight.
- Reasonable care must be taken when moving around an academy site; a device must be transported in a protective sleeve or case (provided by the Trust) to minimise damage.
- Never allow another user outside of the Trust to use the device. This includes family, friends and other third parties. To do so increases the risk of a data breach and can have serious implications for the Trust.
- The device should not be connected to the mains constantly as this damages the charging ability of the battery and will reduce its lifespan considerably. Instead the device should be allowed to complete charge and discharge cycles.
- Always lock your device when leaving it unattended. For Windows devices this can be simply done by pressing the Windows Key + L
- The device should be restarted at least once per week to allow for updates to install. For Windows devices press the Shift Key + Shutdown Option.
- Care should be taken when inserting or removing cables. Broken ports are not covered by warranty.
- Never leave the device unattended and unlocked.
- Try to minimise using public Wi-Fi hotspots as they can be less secure and have snooping devices attached.
- If you do use a public Wi-Fi hotspot, ensure you set your device to forget it once finished.
- Do not make any attempts to circumvent the safeguarding or security settings on the device. In doing so you could be subject to the Trust’s disciplinary policy.
- Do not install peer-to-peer networking clients.
- Do not store personal files (including photographs and music libraries) as this consumes network storage and can shorten the lifespan of the network.
- A screen capture/keyboard logger is installed on each device for safeguarding purposes. It is a disciplinary offence to disable or tamper with this software.
- Any issues relating to software corruption will result in the device being reconfigured.
  This process removes all existing data on the device and restores it to its baseline setting.

Enforcement

Enforcement of this policy lies with the Trust.

Trust Issued Devices (Staff) Agreement

The following are the conditions under which you accept the named device. This agreement will start on receipt of the device from the Trust. The Trust reserves the right to transfer the device to another member of staff if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

Under this Agreement the Trust will:

1. Provide the named device for your sole use while you are a permanent full-time or part-time staff at the Trust. The device is for work use. You are permitted to use it outside work hours in accordance with the Acceptable Use Policy. However, it is for your sole use only, and not for use by pupils, family members or any other person.
2. Set up the device to enable you to connect to and make effective use of the Trust's network, and provide a secure location for the safe storage of your device during the school day e.g. a classroom or office that can be locked.
3. Plan and manage the integration of the device into the Trust's environment, and provide the professional development required to enable you to use the device effectively in your professional practice.
4. When required expect you to pay an excess for accidental damage or loss, or repair/replacement costs where the loss or damage is a result of your own negligence.
5. Have an expectation that you will abide by the Trust's IT policies including the Acceptable Use Policy.

Under this Agreement you will:

1. Use the device for the purposes it was provided and abide by the Trust's policies.
2. Provide suitable care and security of the device at all times and immediately report any damage or loss of the device to the Trust.
3. Be responsible for any software not installed on the device by the Trust, if your device was unrestricted prior to the signing of this agreement. This includes fines for illegal software or files and breaches of copyright.
4. Be prepared to cover the excess or the cost of repair or replacement of the device when the damage or loss has been a result of your own negligence.
5. Make a commitment to achieving the IT goals of the Trust and take part in the IT professional development activities provided for you by the Trust.
6. Make necessary arrangements for the return of the device to the Trust when you resign or leave the Trust or when you will be away from the Trust for an extended period or when requested to do so for necessary IT maintenance tasks.
7. In accordance with Trust policies, be held responsible for any involvement by yourself or any other user of your device in activities associated with accessing inappropriate or illegal materials.

Device Details

School:

Make & Model:

Serial Number:

I have received the above device in good working order and accept the conditions of the loan:

Staff Name:

Signature: **Date:**

Appendix 4 – Trust Password Guidance

- Do not write passwords down, the Trust encourages use of password safes for this purpose, and recommends LastPass.
- Use a 10 character password which includes upper and lower case characters, symbols and numbers
- Do not use a proper word or name as your password, even if using upper and lower case, symbols and number in it
- Consider using 4 short random words as your password, i.e. dogshieldcargrass. Then add random symbols etc. d0g3Hie1d(argR@ss This provides a higher level of protection from cyber actors.
- Don't use pets, businesses, family, friends etc.
- Don't use birthdays, wedding days, addresses, or post codes
- Don't use number or letter sequences (1234, abcd)