JOHN TAYLOR MULTI ACADEMY TRUST

ICT Security Acceptable Use Policy

Implementation date: January 2018

Review date: November 2023

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	01/04/2017	First Draft
1.1	M. Crompton	23/11/2017	Inclusion of other policies and agreements to create a single policy with appendices.
1.2	M. Crompton	27/09/2018	Implement changes around the wording of the document and the introduction of examples/ citations.

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, third parties, students, 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 John Taylor Multi-Academy Trust. The 'appropriate level of authority' should be determined according to the employer's decision making structure. This policy applies any users whom have access to the network, 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 of the Trust.

Acceptable Use

All users, devices and connectivity services

1. When logging on to the network, user must always use their own username and password.
2. Any user who identifies a security problem on the Trust's network must notify IT Services immediately.
3. Users must follow the Password Policy. 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 IT Services.
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.

6. Users must understand that the information they hold on the network is not private and can be inspected at any time. Examples when this might occur include, but are not limited to:
   a. A safeguarding concern is raised via the appropriate channels
   b. Your disk space usage is high or exceeding our limits
   c. A virus has been detected by the IT systems
7. Users must understand the network employs several monitoring technologies to record access to the internet, keystrokes and catalogue open windows.
8. Users must not store personal documents/pictures/music on the Trust's network.
9. Before leaving a device, users must always log off or lock their device and check this procedure is completed.
10. Users must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
11. It is strictly forbidden for users to attempt to share drives, folders or files across the network via methods not approved by the Trust[1]. File sharing via Peer to Peer software or the running of personal servers is strictly prohibited[2].
12. Only software that has been provided by IT Services may be run on the computers unless prior consent from the Strategic Network Manager it obtained. Users are not permitted to import or download applications or games onto shared machines[3].
13. Students 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).

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 details of another remember 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 in or on insecure devices or locations. Data of this type can be accessed via SIMS or Go4Schools, therefore paper copies of lists and/or other pupil data are actively discouraged and should not be taken home.
4. Staff should ensure devices connected to trust accounts are kept secure whilst in and out of school and report any loss to IT Services immediately.
5. Staff must not store school/trust material on cloud folders (excluding Office 365), USB pens or external hard drives if they are not encrypted.
6. Do not disclose personal or sensitive data to third parties, including app developers[4] without written authorisation from IT Services or their line manager.

[1] Approved methods include the staff/student shared areas, Office365 and paid for applications such as MyMaths, Show My Homework and Linguascope.
[2] Example of peer to peer software/technology would include BitTorret.
[3] This will not be applied retrospectivity and instead will apply from the point the document was signed
[4] Software that has been configured by IT Services will be configured by default to prevent this. Any concerns should be reported to IT Services as soon as possible.

Devices

Some users are provided with either a dedicated device for the betterment of their teaching and learning and/or administrative duties. These devices will be fully supported and maintained by IT Services and personal devices will be supported in connecting to Trust services. By accepting the provision of a laptop/mobile device, users agree to and sign the appropriate JTMAT document detailing our expectations. See Appendix 3 & 4 for the appropriate agreement.

Personal Devices

1. When users are connected to the JTMAT 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 in 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 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 these 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 hacking, encryption and other system tools[5] are expressly forbidden.
4. Users must not engage in activities that are prohibited under UK 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 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 the appropriate of this policy or agreement may result in disciplinary action being taken by the Trust. This responsibly can be delegated to Local Governing Bodies (LGBs) or school leaders depending on the type of breach or the stakeholder(s) involved.

[5] System tools include but are not limited to Command Prompt, Powershell, Regedit and MMC Snapins

Appendix 1 – Acceptable Use Policy Agreement

John Taylor
Multi Academy Trust

Acceptable Use Policy

Version: 1.4

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	13/02/2017	First Draft
1.1	M. Crompton	01/04/2017	Added expectations follow GDPR course
1.2	M. Crompton	27/04/2017	Amendments to SPAG and content in consultation with IT Services
1.3	M. Crompton	05/05/2017	Amendments following CEO consultation
1.4	M. Crompton	22/11/2017	General amendments prior to submission

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): _____

Tutor Group (if applicable): _____

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

Signature: _____

Date: _____

Parent/Guardian – Acceptance (Students 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 my son or daughter or the child in my care to use and access the trusts 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 a secure environment but the trust cannot be held responsible if a students action is in breach of the this AUP.

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

Name of Parent/Guardian: _____

Parent/Guardian Signature: _____

Date: _____

Appendix 2 – WiFi Registration (Staff & Students)

John Taylor
Multi Academy Trust

Acceptable Use Policy
WiFi Registration (Staff & Students)

Version: 1.3

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	13/02/2017	First Draft
1.1	M. Crompton	27/04/2017	Amendments to SPAG and content in consultation with IT Services
1.2	M. Crompton	22/11/2017	General amendments prior to submission
1.3	M. Crompton	12/01/2018	Amendments to formatting

Agreement

The Trust is responsible for the implementation of this policy. However, it may chose delegate this responsibly to Local Governing Bodies, school leaders or IT Services. This document can only be actioned 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 be a current student or member of staff. 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 IT Services office. Once received your request will be processed within 1 working day. Confirmation will then be sent to your school email account.

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
- Remove any Peer-to-peer file sharing programs e.g. BitTorrent

Failure to maintain a virus/spyware free 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 students 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 polices 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 students 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 of the ICT systems, email, internet and other digital communications.

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, spyware, 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 the equipment
5. Attempting to access unauthorised areas of the network
6. Accessing inappropriate web sites or trying to circumvent the school's systems. 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 behaviour or discipline policy. The Trust may delegate this responsibly to Local Governing Bodies or school leaders. If suspected illegal activity has taken place the relevant authorities (e.g. Police) will be contacted.

John Taylor
Multi Academy Trust

Acceptable Use Policy
WiFi Registration (Staff & Students)

Version: 1.3

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 copy of the **Acceptable Use Policy** signed.

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.

Staff and Students to complete

Name: _____

Trust Email Address: _____

Signature _____

Date: _____

Students Only (Including 6th form)

Students are required to obtain permission from their parent or guardian before use of the Trust's WiFi network can be granted.

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Date: _____

Please bring this completed document to the relevant IT Services office.

Appendix 3 – Trust Issued Devices (Staff)

John Taylor
Multi Academy Trust

Acceptable Use Policy
Trust Issued Devices (Staff)

Version: 1.5

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	13/02/2017	First Draft
1.1	M. Crompton	01/04/2017	Added expectations follow GDPR course
1.2	M. Crompton	27/04/2017	Amendments to SPAG and content in consultation with IT Services
1.3	M. Crompton	05/05/2017	Amendments following CEO consultation
1.4	M. Crompton	22/11/2017	General amendments prior to submission
1.5	M. Crompton	12/01/2017	Amendment to SPAG and content (Audit committee)

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. IT Services must balance the need for educational freedom that a device can bring alongside the requirements set out in 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 IT Services and what access you will have to the device.

The Device

IT Services procure 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. This specification is decided by IT Services who have the appropriate knowledge.

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 this cost (time and part) will be allocated to the appropriate cost centre via the normal ordering procedures.

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

Access to the device

IT Services 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 IT Services) 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 IT Services 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 for insurance purposes.
- Reasonable care must be taken when moving around an academy site; a device must be transported in a protective sleeve or case (provided by IT Services) 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 month 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.
- Refrain from using public Wi-Fi hotspots as they can be less secure and have snooping devices attached.
- Do not make any attempts to circumvent the 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, although it may choose to delegate this responsibility through Local Governing Bodies or school leaders, depending on the nature of any breach and the stakeholder(s) involved.

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 School 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. However, it is for your sole use only, and not for use by students, 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 IT 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.
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

Home Academy/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 Issued Devices (Students)

John Taylor
Multi Academy Trust

Acceptable Use Policy
Trust Issued Devices (Students)

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	13/02/2017	First Draft
1.1	M. Crompton	27/04/2017	Amendments to SPAG and content in consultation with IT Services
1.2	M. Crompton	22/11/2017	General amendments
1.3	M. Crompton	12/01/2018	Amendments to SPAG and page numbering (Audit Committee)

Trust Issued Devices (Students) Agreement

The person whose name and signature appear below has read and accepts the responsibilities laid out within this document regarding the loan of a computing device owned by John Taylor Multi Academy Trust. A copy of this document is to be retained by the student's parents/guardians.

The computing device provided is **NOT** covered by any insurance policy, so special care needs to be taken in looking after the device. . The Trust will not be liable for any faults, repairs or damage where the device has not been properly looked after in accordance with this agreement or the manufacturer's guidelines.

In receiving the computing device on loan from the trust, the person to whom it is lent agrees:

1. To take all reasonable care for its security from damage and theft (e.g. it will not be left in an unlocked classroom) and will be stored out of sight whilst travelling to and from trust premises.
2. To be responsible for resolving any repairs or software licence issues arising for the duration of the loan.
3. To take responsibility for knowing at all times where the computing device is.
4. To bear herself/himself any costs arising from connection to the Internet.
5. To return the device including power adaptors, case and any other peripherals/accessories loaned with the device when requested, to the Trust and in any case before leaving the Trust.
6. The Trust will NOT maintain the computing device or repair faults not covered by the warranty (if applicable).
7. In the event of accidental damage to the device or loss due to theft etc, to bear the cost of repair or replacement.

Person handing over the computing device	:
Type of device being lent	:
Device serial number	:
Date of loan	:
Student Name	:
Warranty Expires On (if applicable)	:

I have received the above described computing device in good working order and accept the conditions of this agreement:

Student Signature : _____ Date: _____

I the Parent/Guardian of the above named student accept the conditions of this agreement. I also agree that if the device suffers accidental damage or loss due to theft, I will bear the cost of the repair or replacement. Any such loss or damage should be reported to the Trust as soon as possible.

Parent/Guardian Name : _____ Date: _____

Parent/Guardian Signature : _____