Trinity Multi Academy Trust

Policy:	Acceptable Use of ICT (workforce) policy (Encompassing acceptable internet use)
Date of review:	June 2018
Date of next review:	June 2020
Lead professional:	Director of ICT & Data Systems
Status:	Non-Statutory

Empathy, Honesty, Respect, Responsibility

1. Purpose of policy and guiding principles

1.1. The purpose of this document is to provide all establishments within the Trust with a policy, and procedures, that the Board of Directors have adopted to make clear standards and expectations of all staff, in relation to using technology resources.

1.2. The purpose of this policy is:

1.2.1 to comply with statutory requirements, in respect of safeguarding

1.2.2 to ensure that all employees are aware of the Trust expectations, in relation to using ICT equipment and resources.

1.2.3 to clarify the conditions under which resources are provided

1.2.4 to clarify the purpose of providing resources

1.2.5 to make employees aware of implications of abusing Trust resources

1.2.6 to provide guidance to ensure that staff are protected from potential allegations of misuse, or misconduct.

1.3. Throughout this policy references are made to "technology", "ICT systems" and "ICT resources or equipment". These terms are interchangeable and all refer to the services and devices supplied or managed by the Trust ICT team.

1.4. ICT resources include; Internet services, all other electronic or telephony communications, hand held devices, email accounts, VLE (Virtual Learning Environment), desktop PC's, laptops, cameras and tablets. This list is not exhaustive and staff will recognise that advancements in technology make it difficult to list all current, and future, resources or technology services that are covered by this policy.

1.5. This policy applies to all employees, Directors and Governors, volunteers or supply staff who have authorised access to Trust ICT resources.

1.6. Employees will appreciate that any abuse of ICT resources or failure to follow expectations and standards outlined in this document may lead to disciplinary action being taken.

1.7. The Trust reserves the right to request re-imbursement of costs, should an employee abuse, lose or misplace ICT equipment or resources. (i.e. unauthorised telephone calls).

1.8. On leaving employment individuals are required to return all Trust resources. See. 1.7.

1.9. The policy also recognises best practice in seeking to maintain good working relationships between staff and management and the operational needs of the Trust, and outlines training, support and guidance that employees can seek to ensure high standards are maintained.

2. Links with other policies or legislation

2.1. Trinity Multi Academy Trust will treat all employees equally and consistently, in accordance with the Trust's Equality Statement.

2.2. This policy links with the academy's Child Protection and safeguarding policies and the Staff Code of Conduct.

2.3. Employees should also be aware that abuse of ICT resources could result in disciplinary action. This policy links to:

- The Data Protection Act 2018 and GDPR 2018 (Relating to the use of personal information)
- The Computer Misuse Act 1990 (Relating to unauthorised access and creation or distribution of computer viruses)
- The Copyright Designs and Patents Act 1988 (which relates to unauthorised copying often referred to as software piracy).

Breach of any of the above could constitute a criminal offence. Where the Trust believes a criminal offence has taken place, it has a duty to inform the Police. Using the Trust resources illegally will be considered as gross misconduct under the academy's Disciplinary Procedure.

2.4. In addition, some abuse may lead to criminal action if illegal material or activity is involved. This will also be considered as gross misconduct under the academy's Disciplinary Procedure.

3. Consultation

3.1. The recognised Trade Unions have been informed of this policy
3.2. The policy was approved by the Board of Directors after consultation and agreement with the recognised Trade Unions.

4. Policy and procedures

4.1. All employees have a duty of care for ICT equipment and resources and are expected to take reasonable steps to maintain the security and safety of any equipment and data. This includes storing securely, using password and PIN codes appropriately (see section 5).
4.2. Any loss or damage to equipment must be reported to the ICT team as soon as possible.
4.3. Any repairs to ICT equipment must be carried out by personnel authorised to do so by the ICT support service.
4.4. The same behavioural and professional standards are expected with electronic communication as are the case with traditional written communication, the telephone and face to face meetings. Staff should consider their online presence on social networking sites, blogs, wikis and micro-blogs such as Facebook and Twitter, in respect of these professional standards. Staff are reminded that any written communication may be used in court should it be required.
4.5. It is acknowledged that the level of ICT knowledge and skills varies amongst staff, and some staff maybe unsure as to what contravenes the standards expected of the Trust. If you are in any doubt about your actions in relation to ICT use, you should refer to:
- your line manager
- a member of the ICT Support service
- a member of the HR support service

4.6. ICT training and support will be offered regularly through the Trust CPD policy and programmes.
4.7. Acceptable internet use policy is outlined in **Appendix 1.**
4.8. Acceptable use of mobiles and hand held technology is outlined in **Appendix 2.**
4.9. The Staff code of conduct is outlined in **Appendix 3.**

5. Security and Controls

5.1. Where a password is required, this must not be shared with others, written down, or easily accessible to others.
5.2. Under no circumstances must attempts be made to access individual log on details, or passwords. This applies to staff and student accounts.
5.3. Where there is a facility for a password, or additional security (i.e. mobile phone passcode), this must be utilised and set up.
5.4. When a PC is not in use for however short a time and whilst ever devices will lockout when unattended, staff must lock their system to ensure information remains secure and prevent potential abuse e.g. malicious acts.
5.5. **Appendix 4** provides more information on passwords and security, and gives guidance as to how to choose a secure password.

6. Roles

6.1. The role of the Principal(s) (for other establishments please read Head in lieu of Principal)
6.1.1. The role of Principal is to ensure that the policy is applied fairly and consistently within their establishment in the Trust.
6.2. The role of the Board of Directors and Local Governing Boards
6.2.1. The Local Governing Board will monitor and evaluate policies in line with statutory and best practice guidelines.
6.2.2. The Board of Directors will review policies in line with changes to legislation and the trust policy review cycle.
6.3. The role of the employee/other staff

6.3.1. The ICT Support service in conjunction with safeguarding staff will oversee detailed monitoring of internet and technology usage, in line with this policy and report any findings to the appropriate senior leader.
6.3.2. The HR Manager and Compliance Manager will advise the Senior Leadership Group on allegations against a member of staff, in relation to this policy.
6.3.3. Employees are responsible for exercising professional judgement when using Trust ICT resources.
6.3.4. Employees are responsible for reading and complying with the requirements of this policy.
6.3.5. Employees are responsible for usage on their own account, and as such protect their security.
6.3.6. Employees are responsible for reporting any breaches of this policy or misuse of ICT resources to their line manager, or appropriate senior leader.
6.3.7. Employees are responsible for seeking support, guidance or access to training if they are unsure of any aspect of their responsibilities within this policy.

7. Monitoring and Evaluation

7.1. The ICT Support service in conjunction with the safeguarding teams will monitor all internet and computer usage across the Trust.
7.2. The Director of ICT & Data Systems will review this policy.
7.3. The HR Manager and Compliance Manager will monitor any allegations, or suspected abuse of ICT resources, in line with the disciplinary policy.
7.4. Any concerns will be bought to the Principal (or Head) in the first instance.
7.5. Any reviews to the policy will be consulted on, and brought to the Board of Directors.

Date adopted by Board of Directors	**June 2018**
Date for full implementation	**June 2018**
Date for review	**June 2020**
Lead Professional	**Director of ICT & Data Systems**
Notes:	**Reviewed – no significant changes**

Appendix 1

This appendix details Acceptable Internet Use Policy

1. Introduction

1.1 The internet is now an essential tool in our daily working lives, for the protection of the Trust, staff and students it is necessary to outline expectations and standards in relation to internet use. Staff should read these standards carefully and in conjunction with the Staff Code of Conduct for ICT (Appendix 3).

1.2 Abuse of the internet may lead to disciplinary action being taken.

2. Acceptable uses of the internet

2.1 As a general principle internet access provided to staff, by the Trust, to support work-related activities. The following list is not intended to be definitive, but sets out broad areas of use that the academy considers to be acceptable uses of the internet:

- To provide communication within the Trust via email, the VLE, MIS and through remote access.
- To provide communication with other schools and organisations for educational purposes via email, the academy website and other approved web tools.
- To communicate, via the Trust e-mail system, acting on behalf of the academy, where an individual has the authority to send the message.
- Any other activities that directly support student learning activities and functions.

3. Unacceptable uses of the internet

3.1 The following list is not intended to be definitive, but sets out broad areas of uses that will be regarded as not acceptable:

- Use for racial, sexual, homophobic or other harassment
- Use of non-educational games
- To access pornographic, obscene or illegal material
- To solicit personal information with the intent of using such information to cause emotional or physical harm
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- To communicate, via e-mail, acting on behalf of the Trust, where an individual does not have the authority to send the message
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this is covered under a commercial agreement or licence
- Hacking into unauthorised areas
- Publishing confidential or sensitive information, defamatory or knowingly false material about Trinity Multi Academy Trust, colleagues, partner organisations and/or students on social networking sites, blogs, wikis or any other online publishing format
- Distributing confidential or sensitive information, defamatory or knowingly false material about Trinity Multi Academy Trust, colleagues, partner organisations and/or students
- Undertaking deliberate activities that affect access to the network or other academy resources
- The deliberate introduction of any form of malicious software into the Trust network or any Trust device
- Use of any bit-torrent, peer-to-peer or other file sharing systems
- Use for personal or private business purposes at inappropriate times. See section 4 below.

4. Personal use of the internet

4.1 Reasonable use of the academy's internet is permitted, providing that:

- It does not interfere with work performance or divert employees from their duties
- It is not used for furthering outside business interests or for personal monetary gain
- The use of the internet conforms with all other acceptable uses of ICT resources
- Usage does not adversely affect the performance of Trust's networks and systems.

4.2 In addition employees should be aware that personal usage of the internet must:
- Be outside working or contracted time
- E-mails sent from personal accounts must not include sensitive, offensive or material that others could consider distasteful.

5. Netiquette

5.1 The following general principals should be adopted in all forms of on-line communication:
- Be polite. Do not be abusive in messages to others
- Use appropriate language
- Do not disrupt the use of the internet by other users. This would include downloading large files and other high volume activities, such as video streaming
- If an employee receives emails, or other communication that they consider to be offensive, or containing inappropriate material, they must report this to their line manager, or a senior leader.

6. Email Netiquette

6.1 The following principals should be applied to the use of the Trust email system:
- Every user is responsible for email sent from their email address
- Only Trust email addresses should be used to conduct Trust business, this would include communication with students and parents
- All email communication with students should be through their academy email address
- Any attempt to read, delete, copy or modify the email of other users is prohibited
- Attempts to send junk mail and chain letters are prohibited
- All email created should be signed with the appropriate email signature
- If you receive email from outside of school that you consider to be offensive or harassing speak to your line manager
- You should be aware that in the event of the Trust being involved in legal proceedings, any relevant emails may have to be disclosed, including internal email.

7. Training and support

7.1 Every attempt is made to prevent access to unsuitable sites, and it is individual's responsibility to respect this. However, there may be occasions where, for learning purposes, sites need to be accessed. Please contact the ICT support service to gain the relevant permissions.

7.2 To support ongoing monitoring, staff are required to report to the ICT team, any sites where access should be restricted, or cause concern.

7.3 It is acknowledged that the level of ICT knowledge and skills varies amongst staff, and some staff maybe unsure as to what contravenes the standards expected of the academy. If you are in any doubt about your actions in relation to internet use, you should refer to:
- your line manager
- the ICT Support Service
- the HR Manager
- the Compliance Manager.

8. Disciplinary action

8.1 As outlined in the main policy, disciplinary action may be taken if these standards and expectations are not followed and if any policy is contravened.

Appendix 2

This appendix details acceptable use of telephones, mobile, or hand held technology, (including laptops and tablets).

1. Introduction

1.1. The Trust can issue mobile phones, iPads or other mobile technology for business purposes.
1.2. In general, the criteria for issuing these resources will be where issuing the equipment;
- Promotes work-life balance
- Ensures that key employees can be reached in case of an emergency
- Supports student learning
- A financial benefit of using mobile technology.

2. Personal use of Trust ICT resources

2.1. Reasonable use of academy's ICT resources and technology is permitted, providing that:
- It does not interfere with work performance or divert employees from their duties
- It is not used for furthering outside business interests or for personal monetary gain
- The use of the internet conforms with all other acceptable uses of ICT resources
- Usage does not adversely affect the performance of the Trust's networks or systems.

2.2. In addition employees should be aware that personal usage of resources must:
- Be outside working, or contracted, time
- Should not be excessive, and any private calls must be reasonable (in terms of length and cost). Please be aware that the academy reserves the right to reclaim any reasonable costs if this policy is abused.

3. Use of personal equipment

3.1. Employees are able to use their own technology or mobile phones during the day. This is providing that usage is outside working time unless absolutely necessary.
3.2. Mobile phones should be kept on silent, or vibrate, during the working day.
(Please refer to the Bring Your Own Device Policy for details of requirements and expectations regarding use of personal equipment)

Appendix 3

This appendix details the Staff Code of Conduct that all staff are required to acknowledge, sign and follow during their employment.

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the Acceptable Use of ICT (staff) Policy, available in the Staff Handbook on the VLE, for further information and clarification.

- I understand that it is a criminal offence to use any Trust ICT resource for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones; PDAs, digital cameras email, and social networking and that ICT use may also include personal ICT devices when used for academy business.
- I understand that academy information systems may not be used for private purposes without specific permission from the Principal.
- I understand that my use of academy information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will log off or lock the computer I have been using when leaving it unattended.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in the academy, taken off academy premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to a Designated Child Protection Officer or a member of SLG.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I will only utilise the Trust email platform to communicate with pupils.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The Trust may exercise its right to monitor the use of information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: .....

Name: ..... Date: / /

Appendix 4
This appendix details the Trust Password Policy

1. Introduction

1.1 Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of academy resources.

1.2 The scope of this policy includes all staff and contractors who have access to Trust systems and who have, or are responsible for, an account that accesses any Trust systems or data.

1.3 Those with accounts are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1.4 The purpose of this policy is to provide guidance as to the standards required for creating strong passwords, the protection of those passwords, and the frequency of change.

2. Policy

2.1 General Password Guidelines

All users should be aware of how to select strong passwords that are used for access to all Trust systems. Strong passwords should have the following characteristics:

- Contain at least three of the following five character classes
  - Upper case characters
  - Lower case characters
  - Numbers
  - Punctuation
  - Special characters (e.g. @#£$%)
- Contain at least 8 characters

Weak passwords include words found in the dictionary, the names of family members, pets, friends, birthdays, phone numbers, addresses and commonly found letter or number patterns (e.g. qwerty, 123321)

2.2 Frequency of Changing Passwords

All system level passwords must be changed at regular intervals as requested; this would include accounts that give system level privileges through group membership through programs such as SIMS. All user-level passwords should be changed on at least an annual basis.

2.3 Password Protection Standards

- Always use different passwords for work accounts from other personal accounts
- Where possible try to keep passwords unique to each service or system.
- Do not share passwords with anyone, including administrative assistants.
- All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g. "my family name").
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the ICT Support service.
- Always decline the use of the "Remember Password" feature of applications.