The Futures Trust

Staff and Volunteer

ICT Acceptable Use Policy

Lead reviewer: I Neal, ICT Director
Approval: Finance, Resources, Audit and Risk Committee
Approved for implementation: April 2017
Date of Review: April 2019 or earlier in response to statutory changes

ICT Acceptable use Policy Index

1. Policy statement

The Trustees of The Futures Trust and the Governing Body support the appropriate use of Information Communication Technology (ICT) and are committed to delivering access to ICT facilities and systems which are secure, enhance the work of staff and volunteers, enrich learning opportunities for students, encourage discussion and creativity and support the achievement of work life balance.

This policy applies to staff and volunteers; there is a separate ICT Acceptable Use Policy that applies to students.

In return they require all staff and volunteers to be responsible users, and in doing so will set and communicate clear expectations supported by the delivery of relevant training.

The Trustees and Governing Body recognise that the appropriate and safe use of ICT facilities and systems, both in the workplace and external to it, is integral to everyone's responsibility to safeguard children and young people. They also recognise that their use can pose a risk to the confidential information we process and store, to the reputation of the Trust, its Schools, individual staff and volunteers, and to the ability of the Trust to deliver an outstanding education for all.

This Policy sets out the standards of conduct required of all staff and volunteers in accessing and using the School's ICT facilities and systems, and where relevant the standards of conduct required external to the workplace. It is intended to ensure that:

- Control measures are implemented to eradicate or minimise the recognised risks;
- Facilities and systems are protected from accidental or deliberate misuse that could put their security, the security of users and the security of information at risk; and
- Staff and volunteers are aware of the risks and the standards of conduct required of them, and will be responsible and stay safe whilst using ICT for educational and personal use.

The Trustees are committed to empowering the Trust's Schools to protect and educate the whole Trust community in their use of ICT, and to establishing mechanisms, including the use of appropriate filtering and monitoring systems, to identify, intervene and where necessary escalate incidents of misuse, whilst protecting the rights and privacy of individuals.

2. Scope

2.1 Terminology

In this Policy and in the Acceptable Use Agreement:

The term ‘staff’ encompasses employees, officers, consultants, contractors, casual workers, agency workers and teachers on ITT placement.

The term ‘volunteers’ includes all those freely giving of their time to contribute to the work of the Trust and its Schools including Governors, Trustees and Members.

The term ‘ICT facilities and systems’ includes computer equipment, telephones, voicemail, fax, CCTV, copiers, scanners, electronic key fobs and cards, cameras, webcams, USB devices, the internet, intranet, School Virtual Learning Environments, email, all forms of social media and networking sites. This list is not exhaustive.

2.2 Application

This Policy applies to all staff and volunteers who are given access to the School’s ICT facilities and systems, and provides an Acceptable Use Agreement (Appendix B) which is to be read, signed and returned to the School HR Office. This should be signed on joining the Trust and then at the start of every academic year.

The requirements set out in this Policy also apply to the use of School’s ICT facilities and systems out of School, and the transfer of personal data (digital or paper based) out of School.

All staff and volunteers must immediately report any illegal, inappropriate or harmful material or incident that they become aware of via the appropriate channels. Any incidents involving the searching for or viewing of inappropriate, explicit or indecent images, or involving someone who is putting themselves or others at risk through their use of ICT, must be reported as a safeguarding matter in accordance with the School’s Safeguarding and Child Protection Policy.

The Policy itself does not form part of any employee’s contract of employment and may be amended at any time, however it is a condition of use of the Trust’s ICT facilities and systems that users are bound by the Acceptable Use Agreement.

Breach of this Policy or the Acceptable Use Agreement may result in Disciplinary action up to and including dismissal. This Policy will apply and disciplinary action may be taken regardless of whether the breach is committed during working hours, and whether the facilities and systems are owned by the Trust or the user, where use affects the welfare of children or young people or constitutes a risk to the Trust or School.

It is acknowledged that this Policy cannot cover every eventuality or the breadth of issues arising out of the use of ICT. As such the Trust will always have regard to the intent of this Policy in its application to matters which may not be explicitly covered.

2.3 Links with other policies and statutory guidance

This Policy has been developed with due regard to the statutory guidance Keeping Children Safe in Education September 2016 (as amended), Guidance for safer working practice for those working with children and young people in education settings October 2015, the Freedom of Information Act 2000 (as amended), the Data Protection Act 1998 and the Computer misuse Act 1990.

The Policy is linked to the School's Code of Conduct, Safeguarding and Child Protection, E-Safety, Disciplinary, Data Protection, Data Handling and FOI, Anti-Bullying and Dignity at Work, Reference and Whistleblowing Policies, copies of which are available from the School HR Office or can be downloaded from the HR section of the School Portal.

A separate ICT Acceptable Use Policy applies to Students.

3. Policy

3.1 Limited and reasonable personal use

The main purpose for the provision of ICT facilities and systems by the Trust is for use in connection with curriculum delivery, teaching and learning and the running of its Schools. The Trust permits personal use of its ICT facilities and systems by staff and volunteers subject to the following limitations:

a) Personal use must be kept to a minimum, and must not be connected with any use or application that conflicts with their obligations to the Trust, School or Students, with any statutory obligations or with the School's policies and procedures.

Facilities and systems:

b) Can be accessed for personal use to manage essential family and domestic issues outside of working hours (before work, after work or during agreed break times). This does not include the use of Trust equipment or phone lines to make personal telephone or video calls which is not permitted except in genuine emergencies, or where authorised by a senior manager.

c) Must never be used for the purpose of maintaining social contact during working hours.

d) Whether during working hours or external to this, must never be used for participating in online gambling, posting, viewing or exchanging social media messages or any other similar activity, unless legitimately required for work purposes.

e) Must never be used for a personal commercial or profit making purpose, or for other financial gain.

f) As a general rule should not be used for the purpose of storing personal images, documents or information, but employees may use their 'My Documents' folder

to keep a minimal amount of data, provided that the data is consistent with a) above, and is stored separately to work documents.

The Trust accepts no liability for the loss of personal data stored using its facilities or systems, and any data stored in breach of this Policy may be permanently deleted without prior notification.

Staff may request formal authorisation from the Headteacher to allow them additional personal use in connection with training or study.

Where an employee's level of performance is deemed to be affected by unreasonable or inappropriate personal use, other parts of this Policy have been breached, or where unauthorised expenditure occurs, for example as a result of excessive printing, disciplinary action will be taken in accordance with the School's Disciplinary Policy.

Permission for personal use may be withdrawn at any time at the discretion of the Headteacher.

Personal use is monitored in the same way as work use (see section 3.6).

3.2 Equipment

Security and passwords

Staff and volunteers must adhere to the Trust's Password Security Policy contained in Appendix A.

Staff and volunteers must not disable or cause damage to Trust equipment or equipment belonging to others. They are responsible for the security of equipment allocated to or used by them, and must not allow it to be used by anyone in work or outside of work; other than in accordance with this Policy and any additional agreement that they may be asked to sign when a piece of equipment is allocated / loaned.

If leaving a computer terminal unattended staff and volunteers should ensure that they lock their terminal or log off to prevent unauthorised access in their absence.

Desktop computers and cabling for telephones or computer equipment must not be moved or tampered with. Alterations should only be performed by people previously authorised by the ICT Services team and where alterations are still required a call should be logged with the School's ICT helpdesk. Any damage or faults involving facilities and systems must be reported as soon as is practicable.

Staff who have been issued with a laptop or other device / equipment, must sign a declaration to evidence when it has been received by them, for what purpose and the date it is to be returned. Staff must ensure that such equipment is kept secure at all times, especially when travelling, and that passwords are used to secure access to any data stored, to protect confidential data in the event of theft or loss.

Confidential data belonging to the Trust or students must never be stored on a USB device, and when sending highly sensitive or confidential information via email the

information must be in an encrypted attachment or the email itself must be sent in an encrypted format. This includes emails to other schools in the Trust as emails are sent via an external server.

Personal equipment

Personal equipment including but not limited to mobile phones, portable storage devices, cameras and laptops must not be used for storing / processing sensitive or confidential data, or by staff or volunteers (except Governors, Trustees and Members) in a professional capacity, unless formally authorised by the Headteacher / CEO. Where personal equipment has been authorised for use:

- The device must be protected by a secure password at all times.
- The device must be encrypted where possible.
- In order to protect confidential / sensitive data, the Trust retains the right to delete data and/or applications from any device that contains Trust information.
- Devices will require the installation of various applications, as determined by the ICT staff based on the type of device.
- It is the user's responsibility to make sure that the data is securely backed up.

Please note that in certain situations a device may be completely wiped in order to ensure that the Trust can protect its data. If given enough notice, ICT staff can work with you to avoid such action. If you find yourself in such a situation, please immediately contact the ICT staff and your line manager.

Staff and volunteers must only communicate with students and parents / carers using official school systems, and any such communication must be in a professional tone and manner.

Staff and volunteers must ensure that if they bring any personal equipment on to the School site that there is no inappropriate content on it, and that it is not accessed by students at any time.

Any data, including images, which belong to the Trust or students, must only be stored on Trust owned equipment or systems, and must never be uploaded or downloaded to any personal device for any purpose except in a professional capacity by Governors, Trustees and Members.

Personal devices must never be used to take photos or videos of students[1], or to make contact with students, parents or carers in a professional capacity, unless required in

[1] *Making and using images of students using Trust/School equipment requires the age appropriate consent of the individual concerned and their parents/carers. Images must not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the setting have access.*

an emergency, for example to make phone contact whilst on a School trip or visit if School equipment is not available.

Staff and volunteers should not use personal mobile phones during working hours and phones should be switched off or switched to 'silent mode'. Staff may use personal mobile phones during break periods if they are not on duty and are out of sight of students.

Staff and volunteers (except Governors, Trustees and Members) must not use their personal email addresses for work related matters, unless formally authorised by the Headteacher / CEO.

3.3 System and data security

Staff and volunteers must not:

a) Delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the Trust or exposing it to risk.

b) Download, install or attempt to install software from external sources of any type on a machine, store programmes on a computer or alter computer settings unless authorised to do so by the Trust ICT Director.

c) Access, copy, remove or otherwise alter any user's files without their express permission.

Incoming files and data should always be virus checked before they are downloaded using the tools provided on school equipment.

If a staff or volunteer uses a personal mobile device in School in accordance with this Policy, they are responsible for ensuring that any such devices are protected by up to date anti-virus software and are free from viruses.

3.4 Use of email

Email accounts are provided by the Trust for the purpose of conducting the business of the School. The use of the School's email system to solicit, trade or advertise services for private commercial purposes, or the unauthorised advertising of goods and services is not permitted.

Additionally staff and volunteers must not use their Trust / School email address for personal reasons, including but not limited to subscribing to non-work related email lists and the ordering of personal goods and services.

Staff and volunteers should always communicate in a professional manner with and assume that email messages may be read by others. They should not include anything which would offend or embarrass the reader or themselves. Email messages may be disclosed in response to a Data Subject Access Request or in legal proceedings, and deletion from a user's inbox or archive does not mean that an email cannot be recovered for the purposes of disclosure.

When using email staff and volunteers must ensure that they do not create access or pass on material that is abusive, obscene, sexually explicit, pornographic, discriminatory, defamatory, derogatory, hateful, bullying, that incites or depicts violence or terrorist acts, is libellous, breaches copyright or is otherwise inappropriate or represents values which are contrary to those of the Trust.

All incoming and outgoing electronic data is automatically scanned for inappropriate content and threats such as computer viruses and other potentially harmful programs.

Staff and volunteers should exercise caution when opening emails from unknown external sources, or where for any reason an email appears suspicious. If in doubt advice should be sought from the School's ICT helpdesk. Hyperlinks and attachments in emails must not be opened unless the source is known and trusted.

In accordance with the Trust's Reference Policy only the authorised persons identified may provide a reference for a person that has carried out work for the School. School email must not be used by staff or volunteers for this purpose. It will be considered a serious breach of safeguarding policy if they do so and appropriate action will be taken.

Staff should not access another user's email system without permission. The facility to grant email permissions is available in Outlook and it allows you to define the level of access a colleague may have to your email account thus removing the need to disclose your password and ID. All line managers should have permission to view relevant folders in the event of absence due to holiday or ill health.

3.5 Use of internet

Visiting websites

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors.

Staff and volunteers must not access any webpage or files downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. If staff or volunteers accidentally access such a webpage or file then they should immediately report it to their line manager including the circumstances that led to the access.

Downloading and uploading content

Staff and volunteers must never upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others, and must never try to use any programmes or software that may enable them to bypass the filtering systems the School has in place to prevent access to any such materials.

Staff and volunteers should not try (unless they have permission from the ICT Service Team) to make large downloads or uploads (in excess of 50Mb) that might take up internet capacity and prevent other users from being able to carry out their work.

Staff and volunteers must seek advice from the ICT Service Team if they wish to send large files to external organisations (in excess of 20Mb) or multiple other users (in excess of 5Mb).

Responsible use of social media

All staff and volunteers must ensure that they establish safe and responsible online behaviours, and ensure that any communication with students, parents or carers through web based or telecommunication interactions take place within explicit professional boundaries. Staff and volunteers must only communicate with students, parents and carers using official school systems, and any such communication must be in a professional tone and manner.

Staff and volunteers must never send requests to or accept requests from students to communicate via any form of social media, and should not give their personal contact details to students for example e-mail address, home or mobile telephone numbers or details of web based identities. If students locate these by any other means and attempt to contact or correspond with a member of staff or volunteer, they should not respond and must report the matter to the school's Designated Safeguarding Lead.

Staff and volunteers must also ensure that they do not bring the school or the Trust into disrepute through their use of social media. As part of this staff and volunteers must ensure that appropriate privacy and security settings are in place. Staff and volunteers should be aware that even in circumstances where they consider their use of social media to be private, inappropriate actions may still amount to a conduct matter to be managed in accordance with the school's Disciplinary Procedure. Further guidance is provided in the Trust's Code of Conduct and the document 'Guidance for safer working practice for those working with children and young people in education settings' October 2015, both of which are available from the School HR Office.

3.6 Monitoring and Information Gathering

All monitoring will be undertaken in a manner which is fair and lawful, (see Data Protection, Data Handling and FOI Policy) which seeks to avoid any unnecessary intrusion and in circumstances where any adverse impact can be justified.

Any information gathered (including that from monitoring) may be shared in accordance with the Trust's Data Protection, Data Handling and FOI Policy and for the purpose of managing staff conduct.

Active monitoring

As part of the Trust's commitment to safeguarding and delivering systems that are secure, the internet activity of school issued devices and devices that connect to the school network is monitored and reported on, whether they are connected via the school network or any other internet connection.

Keyword usage on school devices and devices that connect to the school network is also monitored.

The responsible person (usually either the Network Manager or the ICT Service Team Leader) will ensure that full records are kept of:

- User IDs
- User logons
- Internet activity against User ID and/or Device ID
- Keyword triggers including prevent keywords
- Security incidents related to this policy

Active monitoring is carried out to monitor and ensure compliance with Trust policy and statutory requirements.

Automatically Gathered

Information is automatically gathered on the following and is not actively monitored, but may be interrogated should the need be identified:

- For each user on the network:
    - Last logon
    - Last password reset
- Logon/Logoff to SIMS
- Audit trails within finance systems and other Trust / school provided systems
- Email header information (subject, date, time, recipients, delivery status)
- USB stick usage
- Applications run

Appendix A

Staff Password Security Policy

A safe and secure username / password system is essential if the Trust's Technical Security policy is to be maintained and will apply to all the Trust's / School's technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Passwords must never be made available by staff or volunteers to anyone else, unless formally authorised by the Headteacher. If so required at any time, staff and volunteers must provide details of their passwords to the Headteacher and return any equipment requested.

Staff and volunteers must not use any other person's username of password without authorisation from the Headteacher.

Policy Statements

- All users will have clearly defined access rights to the Trust's / School's technical systems and devices. Details of the access rights available to groups of users will be recorded by the ICT Service Team and will be reviewed, at least annually, by the Online Safety Group.

- All the Trust's / School's networks and systems will be protected by secure passwords that are regularly changed. Where possible remote access to networks and systems should be protected by two factor authentication.

- The "master / administrator" passwords for the Trust's / School's systems, used by the technical staff, must also be available to the Head teacher / Principal or other nominated senior leader and kept in a secure place e.g. a safe.

- Passwords for new users, and replacement passwords for existing users, will be allocated by the relevant ICT Service Team.

- All users

    - Will have responsibility for the security of their username and password;
    - Must not allow other users to access the systems using their log on details;
    - Must immediately report any suspicion or evidence that there has been a breach of security.

- Users will change their passwords at regular intervals – as described in the staff section below.

- Requests for password changes should be authenticated by the relevant ICT Service Team to ensure that the new password can only be passed to the genuine user.

Staff passwords:

All staff users will be provided with a username and password by the relevant ICT Service Team who will keep an up to date record of users and their usernames. For those users:

- The password must be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- The password must not include proper names or any other personal information about the user that might be known by others.
- Users will be required to change their password at least every 3 months.
- Passwords must not be re-used for 6 months.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords will not be displayed on screen, and will be securely hashed (use of one-way encryption).
- Passwords must be different for different accounts, to ensure that other systems are not put at risk if one is compromised.
- Passwords must be different for systems used inside and outside of the Trust / School.
- The account will be “locked out” following five successive incorrect log-on attempts.

Appendix B

Acceptable Use Agreement

I understand that I must use Trust's / School's ICT facilities and systems in a responsible way to ensure that there is no risk to my safety, the safety of students or colleagues or to the safety and security of facilities and systems.

I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

I have read and understood the School's ICT Acceptable Use Policy and Staff Password Security Policy and agree to use the Trust's /School's ICT facilities and systems (both in and out of school) and my own devices (in school and when carrying out communications related to the Trust / School) in accordance with the requirements stated. I understand that if I am authorised to use my own device for email access and it is lost or stolen, that I should immediately notify ICT staff and my line manager. I understand that if the device is not located and returned to my possession that the device will be remotely wiped and all data may be lost.

I understand that if I breach the Policies, through action or failure to act, this may result in Disciplinary action up to and including dismissal.

I understand that if my action or failure to act affects the welfare of children or young people or constitutes a risk to the Trust or School, disciplinary action may be taken regardless of whether the breach is committed during working hours and whether the facilities and systems are owned by the Trust or me.

Job Title / Position	
Staff / Volunteer Name	
Signed	
Date	

If you are uncertain regarding any aspects of the ICT Acceptable Use Policy or Staff Password Security Policy and have any questions, you must ask for clarification from the School's ICT Department before signing this declaration.