The Futures Trust

Staff and Volunteer

ICT Acceptable Use Policy

Lead reviewer: O Adeyemi, Trust ICT Director
Approval: Finance, Resources, Audit and Risk Committee
Reviewed: July 2023
Next Review: March 2024 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.

Staff and volunteers should read these guidelines carefully, in conjunction with The Future Trust's Information Security Policy.

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 refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection,

Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges

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, Information Security, Reference and Whistleblowing policies. The copies of which are available from the school's HR Office. Alternatively, you can download these from the policies section of the school's HR Support Portal on SharePoint.

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) 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 following:

1) The policy statements stated in section 3.2 ‘Electronic information’ and section 7 ‘Portable Media Devices’ of the Information Security policy. These sections contain information about the storage and encryption of confidential information, safeguarding of information, the security of passwords and the control requirements for the use of removable media devices.

2) Trust’s Password Security Policy contained in Appendix A.

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 and that an up-to-date anti-virus software is installed on the device.

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 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 Head teacher / CEO.

3.3 System and data security

[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.*

Staff and volunteers must adhere to the policy statements in section 8 ‘Anti-Malware’ of the Information Security Policy.

In addition, 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 programs on a computer or alter computer settings unless authorised to do so by the Trust ICT Manager.

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

In addition to the statements below, Staff and volunteers must adhere to section 4.2 ‘Email and Other Electronic Communications‘ of the Information Security policy.

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 programs 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 (February 2022).* Both of which are available within the Policies section of your school's HR Support Pages on SharePoint.

3.6 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Keywords
- Any other electronic communications

The school has put in place a web filtering and monitoring system for this purpose. Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school filters and monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

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

3.7 Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
  - Check the sender address in an email
  - Respond to a request for bank details, personal information or login details
  - Verify requests for payments or changes to information
- Conduct regular phishing email simulations to raise staff awareness of the latest phishing techniques and promote a risk aware culture.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the school will verify this using a third-party audit via the Trust at least annually, to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date:** with a system in place to monitor when the school needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be

- Back up critical data daily and store these backups on cloud-based repositories that are not connected to the school's network and which can be stored off the school premises.
- Make sure staff:
  - Dial into our network using secure remote access channel when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually.
- Work with the Trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement.

3.8 Remote Access

We allow staff to access the school's ICT facilities and materials remotely. This includes cloud-based services such as E-mail Access. Remote access will only be allowed via the secure channels that have been put in place.

Staff will need to enrol for Multi-Factor Authentication to access our systems remotely. For further information and to request access, please contact the ICT Team.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the ICT Manager may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

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.
- 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 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.