E-Safety and ICT acceptable use policy

Formally adopted by Evolution Academy Trust	
On:-	**February 2023**
Chair of Trustees:-	**Drew Whitehead**
Last updated:-	**June 2023**

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the operations of Evolution Academy Trust (our Trust) and it's member academy's, and is a critical resource for pupils, staff (including the senior leadership team), trustees, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the Trust.

However, the ICT resources and facilities used within our schools could also pose risks to data protection, online safety and safeguarding. This policy therefore aims to:

- Set guidelines and rules on the use of trust ICT resources for staff, pupils, parents, trustees and governors.
- Establish clear expectations for the way all members of our Trust and community engage with each other online.
- Support Trust's policies on data protection, online safety and safeguarding.
- Prevent disruption that could occur to through the misuse, or attempted misuse, of ICT systems.
- Support the academy in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our trust's ICT facilities, including trustees, governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our staff code of conduct/disciplinary policy.

2. Relevant legislation and 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 2022
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- **The Trust:** all schools which forms part of Evolution Academy Trust

See appendix 1 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the trust's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the trust's ICT facilities includes:

- Using the trust's ICT facilities to breach intellectual property rights or copyright
- Using the trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the trust, or risks bringing the trust into disrepute
- Sharing confidential information about the trust, its pupils, or other members of the trust community
- Connecting any device to the trust's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the trust's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the trust's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the trust's ICT facilities
- Causing intentional damage to the trust's ICT facilities
- Removing, deleting or disposing of the trust's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the trust
- Using websites or mechanisms to bypass the trust's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The trust reserves the right to amend this list at any time. The central team, or headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the trust's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of trust ICT facilities (on the trust premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the trust's policies on staff code of conduct or the behaviour policy. Staff must ensure they are aware of both policies.

5. Staff (including trustees, governors, volunteers, and contractors)

5.1 Access to trust ICT facilities and materials

The Trust and Academy Leaders and our IT provider provide access to the trust's ICT facilities and materials for trust and academy staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the trust's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact their line-manager immediately.

5.1.1 Use of phones and email

- The trust and each academy provides members of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).
- All work-related business should be conducted using the email address the trust has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the CEO/headteacher immediately and follow our data breach procedures.
- Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the trust to conduct all work-related business.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4, and must not be used for personal matters.

5.2 Personal use

Staff are permitted to occasionally use trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The CEO/headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact/teaching time.

- Does not constitute ‘unacceptable use’, as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
    - Staff may not use the trust’s ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).
    - Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
    - Staff should be aware that personal use of ICT (even when not using trust ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.
    - Staff should be aware that working in schools means professional behaviours are critically important and staff must therefore consider this when using social media, and be aware that in-line with the Trust disciplinary and Safeguarding policies, action may be taken if conduct brings the employer into disrepute, or conflicts with other relevant standards of acceptable use.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Staff must be aware that disciplinary action may be taken if content or comments posted are seen in breach of this policy or other EAT policies.

5.3 Trust and Academy social media accounts

The trust has some official social media accounts, managed by designated staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The trust has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.4 Monitoring and filtering of the trust network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the trust 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
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the academy’s designated safeguarding lead (DSL) and line-manager, as appropriate.

The trust monitors ICT use in order to:

- Obtain information related to trust business
- Investigate compliance with trust policies, procedures and standards
- Ensure effective trust 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

Schools will regularly review the effectiveness of the monitoring and filtering systems within schools.

6. Pupils

6.1 Access to ICT facilities

Computers, equipment and devices in each academy's library, ICT suite or in classrooms are available to pupils under the supervision of staff.

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the academy rules as a banned item for which a search can be carried out – as outlined in the Trust behaviour policy, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from DSL or headteacher.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has, or could be used to:

- Cause harm, **and/or**
- Undermine the safe environment of the academy or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher/DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy.

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of academy

The trust will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on trust premises):

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust or academy's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the trust, or risks bringing the trust into disrepute
- Sharing confidential information about the trust, other pupils, or other members of the trust community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust's ICT facilities
- Causing intentional damage to the trust's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation

- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the trust's ICT facilities as a matter of course.

However, parents working for, or with, the trust in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the trust's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

For parent and community governors, a work email address will be provided by the school and this must be used for correspondence and matters relating to the trust.

7.2 Communicating with or about the trust online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. It is also important parents utilise the appropriate channel, if there are concerns.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the trust through our website and social media channels.

It is essential therefore that any issues are raised with our schools directly, enabling them to address swiftly. Headteachers provide a wide range of channels of communication and therefore request that parents utilise the most appropriate channel.

7.3 Communicating with parents about pupil activity

We will ensure that parents and carers are made aware of any significant online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents in the same way that information about homework tasks is shared. Parents may seek any support and advice from the academy to ensure a safe online environment is established for their child.

8. Data security

Our trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents and others who use the trust's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of our ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the trust's ICT facilities.

Any personal devices using the trust's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the trust's data protection policy.

8.4 Access to facilities and materials

All users of our ICT facilities will have clearly defined access rights to trust systems, files and devices.

These access rights are managed by the headteacher or other delegated staff member.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the headteacher or DSL immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

Our trust makes sure that its devices and systems have an appropriate level of encryption.

Trust staff may only use personal devices (including computers) to access trust data, work remotely, or take personal data (such as pupil information) out of the academy setting if they have been specifically authorised to do so by the CEO/headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the trust's IT provider.

9. Protection from cyber attacks

Please see the glossary (appendix 1) to help you understand cyber security terminology.

We will:

- Work with trustees, governors, staff and the IT provider to make sure cyber security is given the time and resources it needs to make our trust secure.
- Provide annual training for staff 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
- 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**: this will be verified using a third-party audit 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 schools 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 frequently and store these backups on cloud-based back-up systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT provider.
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like trust email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in our Trust 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 plans with the IT provider including, for example, how our trust schools 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 frequently and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- All of our academies work with our IT provider and others, to see what we can improve further.

10. Internet access

The wireless internet connection is secure, provides filtering and clear protocol for different connections. We acknowledge that filtering is not 100% accurate, and regular safe supervision and other checks, enable us to monitor closely all internet access.

10.1 Parents and visitors

Parents and visitors to our schools t will not be permitted to use the WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with our schools in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher, DSL and IT providers monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of our trust.

This policy will be reviewed every two years by Trustees.

The governing board is responsible for ensuring the headteacher implements this policy and suitable training is provided.

12. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection policy
- Behaviour policy
- Staff code of conduct
- Remote education (DfE guidance)
- Mobile phone usage
- Data Protection

Appendix 1: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.