



E-Safety Code of Conduct Policy

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
The Governing Body	
Date adopted:	April 2020
Date reviewed	March 2026
Date of next review	September 2027

Aims:

- To safeguard the welfare of learners and staff
- To ensure security and confidentiality
- To safeguard the facilities and uphold the school reputation
- To provide learners with a safe high quality ICT experience as an essential part of their learning
- To set out the monitoring and follow up procedures of any e-safety breach

Objectives:

- To provide robust, safe internet access for all learners and staff, and identify and manage any associated risks
- To promote and secure the welfare of all learners through clear communication of expectation, protocol and procedure for all users of ICT
- To rigorously monitor and review ICT use and practice by all and take appropriate actions to safeguard the school and its users.
- To teach and communicate to learners what internet use is acceptable and what is not and give clear expectations for Internet use
- To educate all learners in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- To make explicit to learners and staff the procedures for reporting inappropriate and offensive Internet and ICT content

General Statement

Edith Kay School recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and enable learners to achieve. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement safeguards within the school and to support staff and learners to identify and manage risks independently. Monitoring and reporting procedures will be in place to ensure that our environment remains safe. We believe this can be achieved through a combination of security measures, training and guidance plus implementation of our associated policies. In our duty to safeguard learners, we will do all that is reasonable to ensure our learners and staff stay e-safe and to satisfy our wider duty of care.

This E-safety policy should be read in conjunction with other relevant school policies, including Safeguarding learners: Child Protection, the Positive Behaviour Policy, the Anti-bullying policy, the Online safety policy and the Whistleblowing policy.

This policy applies to all learners, staff and all members of the school community who have access to the school IT systems, both on the premises and remotely. Any user of the school IT systems must adhere to and sign a hard copy of the Acceptable Use Agreement (appendix 1 for parents and learner or appendix 2 for staff, governors and visitors).

The E-safety Policy applies to all use of the Edith Kay School internet and electronic communication devices, such as email, mobile phones, games consoles and social networking sites, including images, text and sound. This document will set out the school policy with regards to e-safety, but will also give guidance in dealing with any breaches.

Managing Internet Access to ensure security and confidentiality

School ICT systems security will be reviewed yearly and in the event of a breach.

E-mail

- learners must immediately tell a teacher if they receive an offensive e-mail.
- learners must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to learner email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known and you are expecting an attachment from them.
- The school will consider how e-mail from learners to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate learners in their safe use, e.g. use of passwords.
- Newsgroups will be blocked unless a specific use is approved.
- Learners will be advised never to give out personal details of any kind which may identify them or their location.
- Learners must not place personal photos on any social network space provided in the school learning platform.
- Learners and parents will be advised that the use of social network spaces outside school brings a range of dangers.
- Learners will be advised to use nicknames and avatars when using social networking sites.
- No recommendation will be made by staff to use any social networking sites.

Managing filtering

Edith Kay School will work to ensure systems to protect learners are reviewed and improved. If staff or learners come across unsuitable on-line materials, the site must be reported to the E-safety Officer. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

- Learners need to ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the learners' age.
- Where video conferencing is part of off-site distance learning, it should take place in a room where there is a desk and where the parent / carer / guardian is in the room.
- During video conferencing, it is important that staff and learners wear clothing which is:
 - Appropriate to their role and suitable for the activity
 - Not likely to be viewed as offensive, revealing or sexually provocative
 - Not distracting and does not cause embarrassment or give rise to misunderstanding
 - Without any political or otherwise contentious slogans
 - Not discriminatory

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones, cameras and other handheld devices will not be used during lessons or formal school time except as part of a staff sanctioned educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Sony PlayStation, Microsoft Xbox and others that have Internet access which may not include filtering. These are not acceptable for use during the school day (except in Games Club and under staff supervision. It is not permitted for any games machines to be connected to the school WiFi). Staff will use a school phone where contact with learners is required.
- The appropriate use of Learning Platforms will be discussed as the technology progresses.

(Nabil suggestions - 11.03.26)

- Guidance on the ethical and acceptable use of Generative AI tools (such as large language models) will be provided to learners and staff to prevent academic misconduct and the generation of inappropriate content. Please also see the AI Policy and the ICT & Internet Acceptable Use Policy.
- Procedures are established for the reporting and management of synthetic media incidents (deepfakes) used to harass, impersonate, or damage the reputation of any member of the school community. (CPOMS)
- The school has implemented specific protocols to ensure the security of personal data and intellectual property when utilizing third-party remote learning platforms and cloud-based services eg. Right to Audit-any 3rd Party software, 2FA/MFA, User Roles-assign access levels to data accordingly, encryption of data, a clear policy and process for the timely and secure deletion of data applying relevant legislation.
- The school recognises the importance of digital wellbeing and includes measures to mitigate the negative impact of excessive screen time and social media on the mental health of learners and staff. Please refer to the Mobile Phone Policy.

- Any new Internet of Things (IoT) or networked devices introduced to the school environment will undergo a risk assessment to establish security and acceptable use guidelines prior to connection to the school network.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Appendix 1: Edith Kay Independent School acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, debrief time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Name of Learner:

Signed (learner):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for learners using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of learners on a personal device. Where appropriate, the use of a school device is permitted.
- Share confidential information about the school, its learners or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and Admin Lead know if a learner informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that learners in my care do so too.

Name of (staff member/governor/volunteer/visitor):

Date:

Signed (staff member/governor/volunteer/visitor):

Date: