Edith Kay
Independent School

ICT and Online Acceptable Use Policy

This policy is reviewed annually to ensure compliance with current regulations

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

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for learners, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

Edith Kay School recognises the benefits and opportunities which ICT and 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. The ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Safeguard the welfare of learners, parent/carers, staff and governors by setting guidelines and rules on the use of school ICT resources
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Have robust processes in place to ensure the online safety of learners, staff, volunteers and governors
- Identify and support groups of learners that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching learners safe and effective internet and ICT use
- Ensure security and confidentiality
- Set out the monitoring and follow-up procedures of an ICT breach

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.

The ICT and Online Acceptable Use Policy applies to all use of the Edith Kay School internet and electronic communication devices (such as laptops, Chromebooks, desktop pcs, email, mobile phones, games consoles and social networking sites, including images, text and sound).

This policy applies to all users of our school's ICT and internet systems, including governors, staff, learners, volunteers, contractors and visitors, both on the school premises and remotely. Any user of the school ICT and Internet systems must adhere to this ICT and Online Acceptable Use Policy.

This ICT and Online Acceptable Use Policy should be read in conjunction with other relevant school policies, including Safeguarding and Child Protection Policy, Positive Behaviour Policy, Anti-bullying Policy, Online Safety Policy, Disciplinary Policy and Procedures, Staff Code of Conduct and Whistleblowing 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 2023
- 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
- UK Council for Internet Safety (et al.) 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
- https://www.gov.uk/guidance/plan-technology-for-your-school

3. Definitions

- **ICT and Internet Systems:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, Chromebooks, tablets, phones, music players, hardware, software, websites, web applications or services, software applications and any device system, application or service that 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 and Internet facilities, including governors, staff, learners, 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 systems and facilities, including but not limited to, documents, spreadsheets, presentations, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 3 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school'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 school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its learners, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school'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 school'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 school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school'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 school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

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

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school 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.

Pupils may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed.

Please refer to the Artificial Intelligence (AI) Policy.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's Positive Behaviour Policy, Anti-bullying Policy, Disciplinary Policy and Procedures, Staff Code of Conduct, Online Safety Policy, Mobile Phones Policy and Whistleblowing Policy.

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

5.1 Access to school ICT facilities and materials

The school's admin lead, business manager, and IT adviser manage access to the school's ICT systems, facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, Chromebooks, 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 school's ICT systems ad 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 the admin lead.

5.1.1 Use of phones and email

The school provides each member 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 school has provided.

Staff must not share their personal email addresses with parents/carers and learners, 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 admin lead immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or learners. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

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.

5.1.2 Managing video conferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Staff must supervise video conferencing and ensure the content/discussion is appropriate for the learners' age.
- During video conferencing, it is important that staff 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

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Head Teacher 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 time/teaching hours/non break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no learners are present
- Does not interfere with their jobs, or prevent other staff or learners from using the facilities for work or educational purposes

Staff may not use the school's ICT systems and 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 systems and 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 school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where learners and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see child protection and safeguarding, online and mobile policy) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

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.

The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

5.3 Remote access

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 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.

5.4 School social media accounts

The school 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.

5.5 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 systems, 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 school 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 adviser, as appropriate.

Cheat sheets for some of the various social media platforms are in Appendix 2, with information on how the platforms are used, their pros and cons, and how to help keep young people safe.

6. Learners

6.1 Access to ICT systems and facilities

Computers and equipment at the school are available to learners only under the supervision of staff

- Specialist ICT equipment, such as that used for design and technology, must only be used under the supervision of staff
- Learners will be provided with an account linked to the school's virtual learning environment, which they can access from any device by logging into their school Google account

6.1.1 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.
- 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.

6.1.2 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.

Cheat sheets for some of the various social media platforms are in Appendix 2, with information on how the platforms are used, their pros and cons, and how to help keep young people safe.

6.1.3 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 learners wear clothing which is:
    - Appropriate 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

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 learners 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 learners, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **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 learners and staff. If the search is not urgent, they will seek advice from Headteacher/DSL.
- Explain to the learner why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the learner's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a learner was in possession of a banned item. A list of banned items is available on the behaviour policy
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

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 been, or could be, used to:

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/Head Teacher/SLT 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 whether there is a good reason to erase data or files from a device, staff members will consider whether 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 is 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 learner 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) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy. Please refer to DfE guidance.
- Any complaints about searching for, or deleting, inappropriate images or files on learners' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction learners, in line with the Positive Behaviour Policy, if a learner engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school'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 school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other learners, or other members of the school 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 school's ICT facilities
- Causing intentional damage to the school'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
- Please refer to the Positive behaviour policy.

7. Parents/carers

7.1 Access to ICT facilities and materials

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

However, parents/carers working for, or with, the school 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 school's facilities at the headteacher's discretion.

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

7.2 Communicating with or about the school online

We believe it is important to model for learners, and help them learn, how to communicate respectfully with, and about, others online.

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

7.3 Communicating with parents/carers about learner activity

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

When we ask learners to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school learners will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

Cheat sheets for some of the various social media platforms are in Appendix 2, with information on how the platforms are used, their pros and cons, and how to help keep young people safe.

8. Data security

The school 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, learners, parents/carers and others who use the school's ICT systems and 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 school's ICT systems and facilities should set strong passwords for their accounts and keep these passwords secure. Please refer to the online safety policy.

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 learners 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.

All staff will use the password manager required by the Admin Lead/Online Safety Lead/IT adviser to help them store their passwords securely. Teachers will generate passwords for learners using the required password manager or generator and keep these in a secure location in case learners lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's 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 school's ICT facilities.

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

8.3 Data protection

All personal data must be recorded, processed, transferred and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's ICT systems and facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the admin lead.

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 admin lead/head teacher 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

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as learner information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT adviser/consultant.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

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
- 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 (such as 360 degree safe) 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 and store these backups on cloud based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT Technician
- Make sure staff:
- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- 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 every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The school's wireless internet connection is secure. The school use a filtering system which is managed by the IT adviser.

10.1 Learners

Learners will only have access to the school's WiFi when using devices (e.g. laptops and Chromebooks) supplied by the school. All school devices use a filtering system and are monitored by the IT adviser.

Learners are not permitted to have use of the school WiFi on any of their personal devices. Any requests for access to the school WiFi on a learner's personal device will be politely declined by staff.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer)
- Visitors need to access the school's 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 and IT adviser/online safety lead and business monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every three years.

The governing board is responsible for reviewing/approving this policy.

12. Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Positive Behaviour
- Staff discipline
- Data protection
- Remote education
- Mobile phone usage

Appendix 1: Social media cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on social media

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
- Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
- Check your privacy settings regularly
- Be careful about tagging other staff members in images or posts
- Don't share anything publicly that you wouldn't be happy showing your learners
- Don't use social media sites during school hours
- Don't make comments about your job, your colleagues, our school or your learners online – once it's out there, it's out there
- Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
- Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
- Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or learners)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, learners and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A learner adds you on social media

- In the first instance, ignore and delete the request. Block the learner from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the learner asks you about the friend request in person, tell them that you're not allowed to accept friend requests from learners and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the learner persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school

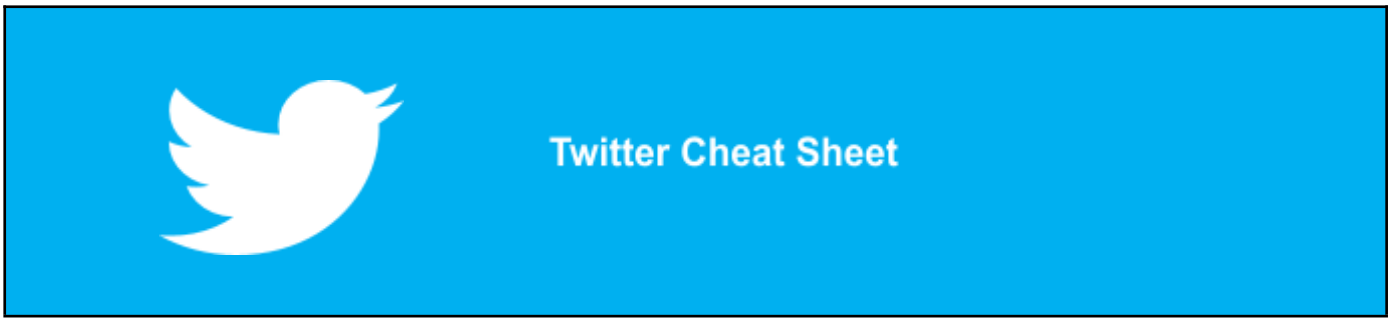
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current learner or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Social media cheat sheets for learners, parents and staff

Pros	Cons	Privacy	Reporting
• Simple to personalise 'feed' – your child can be selective with whom they add or accept as friends, follow only pages they're interested in and join groups of like-minded people. • Easy to hide posts and users they don't want to see or interact with without having to unfriend or unfollow. • Option to categorise or segment their friends list so they can share posts with different groups of people.	• Doesn't validate personal information or photos, so it is easy to pretend to be somebody else or create a new identity altogether. • While the age requirement is 13-years-old, Facebook doesn't check this, therefore allowing children to access the platform at a younger age than it was designed for. • Personal information is readily available – friends can often get access to phone numbers, addresses, school details, photos etc. However, there are ways to address this (see 'Privacy' section).	• Via 'Privacy Settings' your child can customise the visibility of their personal information, photos and posts, choosing from everyone on Facebook, just their approved friends, or no one at all. • Can select who is able to add them as a friend and send them private messages ('everyone', 'friends of friends' or 'no one'), and also whether their profile is searchable using their phone number and email address. • Can easily check and change these settings via the mobile app. (Select 'Privacy Shortcuts' and there are plenty of options)	• Variety of options available to report, block and hide people or posts. More information on what to do if you or your child wants to report something can be found here.



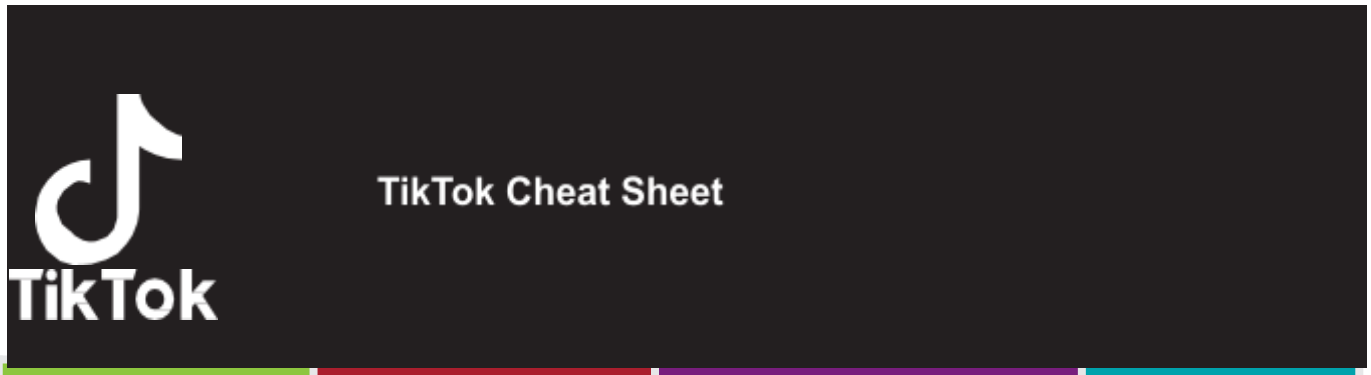
Pros	Cons	Privacy	Reporting
• Limits the amount of information your child can share publically – this includes a short biography, a location and a website. • Trending topics and 'moments' allow your child to join conversations and hear a large variety of viewpoints. If some of these viewpoints contain swearing and inappropriate content, Twitter often censors these. • Ability to mute tweets and accounts that contain certain keywords – more information on this can be found here. • Ability to have a private account where only the followers your child accepts will see their posts.	• No way to validate that anyone is who they claim to be. • Bullying (known as trolling) is particularly prevalent on Twitter. • News updates are not fact-checked, so it is possible that your child may view 'fake news'. This can be countered by encouraging them to use a range of trusted media sources and to ask questions if they don't understand something. • Twitter posts are indexed by major search engines, meaning anything your child posts may be visible to anyone who searches for a keyword included within their tweets, e.g. the name of their school or other personal information.	• All-or-nothing approach – once an account is private, the only information visible to others is their profile and any biography information. Anyone new who wishes to access to their profile has to request to follow them, and no one outside of their existing followers can send them a private message (unless they're messaging someone with different settings).	• Ability to report tweets, moments and users, with categories of violations including irrelevant/not interesting ('I'm not interested in this Tweet'), suspicious or spam, abusive or harmful, expresses intentions of self- harm or suicide. More details about reporting issues on Twitter can be found here. The site also has a section dedicated entirely to child sexual exploitation.

Instagram Cheat Sheet

Pros	Cons	Privacy	Reporting
• Visual way to engage with friends, families, celebrities and influencers – your child can take and edit their own pictures or simply like other people's. • A creative outlet that can allow your child to express themselves and develop new skills and interests. • Ability to have a private account where only the followers your child accepts will see their posts.	• Fake accounts and easy-to-bypass age restrictions are not uncommon on Instagram. • Anyone who clicks a hashtag can see all the public images that have used that hashtag, meaning your child's pictures could be seen by many more users than they intended. • Tagging a location means everyone who clicks that location can see where your child has been and at what time they posted it. This can make it easy to paint a picture about where your child lives or regularly visits. • Instagram Stories (short videos that only last 24 hours) are visible to all users unless profiles are set to private.	• All-or-nothing approach. A private profile only shows photos and videos (including Instagram Stories) to your child's existing followers. Anyone new has to request to follow them.	• Can report spam and abuse within the app. Features a help section for complaints about sexual or nude photo requests and people threatening to share private images, with helpful guidance for under 18s. More information can be found here.

Snapchat Cheat Sheet

Pros	Cons	Privacy	Reporting
• Fun and creative way for your child to keep in touch with friends and family, with simple editing tools and features. • Engaging game-like features, including streaks and winning emoji trophies for completing tasks. • Default privacy settings mean only friends can contact your child or view their story – this can be reduced further to a custom set of friends.	• Ability to screenshot and save images that weren't intended for saving. • Easy to create a fake profile without providing any personal information. • 'Snap Maps' allow your child to share their location very easily. Further, an option called 'ghost mode', which shows all friends' locations except for the user. • Ability to 'quick add' – means you could show up in someone else's 'Quick Add' if you share mutual friends or connections.	• Extensive privacy settings allow your child to control who can see their photos and send them photos in return. These can be changed in the 'Who Can…' section of their profile. See **here** for more on changing privacy settings on Snapchat.	• Can easily report individual 'snaps'. Snapchat requirements mean your child can have other users blocked, but a reason must be stated, i.e. inappropriate photos, harassment etc. Find out more about reporting issues on Snapchat **here** and **here**.



Pros	Cons	Privacy	Reporting
• TikTok is fun and entertaining. It's a video-sharing site that showcases everything from duets and comedy skits to makeup transformations, all of which can be easily searched for using hashtags. It is also filled with fun, colourful, and seasonal graphics. • It provides lots of creative inspiration – great for children and young people who are interested in making their own videos.	• TikTok can feel frenetic. Short videos will play automatically as users scroll through their feeds. Many videos also contain music, so it can be loud and disruptive. • Children can accidentally be exposed to content not intended for them. • Viral "challenges" are big on TikTok. These can encourage dangerous behaviour. • TikTok has made steps to remove inappropriate content (e.g. swearing, drug and alcohol usage, self-harm videos, sexualised content, dangerous challenges), but it can still slip through. You can reduce this threat by clicking 'Restricted' mode within settings.	• After being fined a record $5.7 million for failing to seek age verification or shut down users under 13, TikTok has removed all accounts created by pre- teens, as well as launching a new child-friendly 'kids only' version of the app. In this version, children can still record content but are restricted from uploading it. Other restrictions include not having profiles or access to direct messaging and commenting. Users of the kids' version can still watch videos as usual. • When creating a profile on TikTok, the default settings mean that the profile is public to anyone. This is so users can rack up as many views as possible, gaining popularity. The risks of a public account include: cyberbullying, adult content, grooming. • You can easily switch accounts to private via the **Privacy and Setting** page. You can also restrict interactions (like comments) to 'friends' or 'off'.	• You can easily report an inappropriate video by tapping the share icon and then selecting report. Find out more about **how to report inappropriate content**.

Cheat Sheet

Group Chats

Giving parents and carers everything they need to know about online issues, including insights and experiences direct from young people.

What are group chats?

Group chats are private conversations happening using technology that include more than just two people. You might be familiar with group chats on messaging apps like WhatsApp, but they can also happen on games and social media. Like any conversation, group chats have different purposes including:

- chatting to friends
- messaging family
- planning activities
- asking questions
- passing on information
- sharing photos
- large chats for people with similar interests, such as for a concert or fan groups

Did you know?
Group chats are often set up by children for their whole class or year group to use.

Where are young people having group chats?

Young people use different apps for group chats but for many, their first group chats will be on games like Roblox. Often, WhatsApp is seen as for adults and 'work'. For example, family chats or revision groups. For fun, young people use Snapchat, Instagram and Discord.

"I've always found it's been very much Snapchat for, like, play and then WhatsApp for work." Anna, 17

What do young people like about group chats?

- quick and easy communication
- a place to get help from others
- convenient
- don't have to arrange to meet up or all be free at the same time to hang out
- can dip in and out of conversations
- makes it easy to find links and information
- can help you get to know people before an event or working together. For example, before going to college

What are young people's concerns about group chats?

- online bullying including mean messages or arguments breaking out
- subgroups where certain people are excluded and talked about
- memes, language and comments that are hateful like homophobia, misogyny and racism
- pressure to be active and involved in group chats
- FOMO (fear of missing out) when messages are exchanged when they are busy, including late at night
- sharing of personal information
- a pressure to be funny or controversial
- stigma against those who do not participate
- if you step away, the topic can change and move on leaving you behind
- can include distressing or harmful content such as pornography or non-consensual nude image sharing

What strategies are young people using to manage group chats?

Lots of the young people recognise the challenges of using group chats and are already finding ways to make their experiences more positive. For example:

- using the 'mute' tool to prevent active groups becoming a distraction
- leaving groups they don't want to be part of
- starting new groups if existing ones no longer felt safe
- using settings to prevent people adding them to group chats without permission
- working together to moderate behaviour in chats, for example by having a group admin or issuing warnings to members

Did you know?
Group chats can be of varying sizes and some have hundreds of participants. Young people may be added to group chats with people they know and people they don't.

How can you help?

- Talk to your child about group chats. Start with the positives, but set clear expectations about being kind, respectful and responsible while in group chats.
- Look out for signs that your child's use of technology is impacting their wellbeing. Group chats can be overwhelming, so check in with your child and make sure they know they can always come to you if something is worrying or upsetting them online.
- Discuss how to manage 'online friendships' and contact with people they do not know in person. Strategies like leaving group chats that make them feel uncomfortable, always keeping personal information private, and avoiding chats with unfamiliar 'friends of friends' or 'randomers' are key.
- Familiarise yourself with key settings and support your child to use these too. These could be reporting and blocking tools, muting chats or turning off read receipts.
- Search online for the platforms your child is using with search terms 'privacy settings', 'group chat settings' or 'parental controls' to find the relevant settings available.

Supporting Under 11s

- If your child shows an interest in group chats, remember that most social media apps have an age rating of 13+.
- If your child tells you that all their friends are using group chats, talk to other parents to confirm this, and make a decision that works for you and your family.
- If it's a no, you're not on your own. Many parents prefer to wait until their child is older.
- If it's a yes, supervise and monitor your child's use. Set clear expectations and check in regularly.

Supporting older children and teens

- Spend time with your child ensuring you both know how to use the block and report features, and how to take screenshots (this can help them show you something that may have gone wrong).
- Work together to find a balance that allows you to support and monitor their use of group chats, whilst still giving them some privacy. Expecting to access all their private chats may push your child away or lead to them keeping secrets.

Supporting a 16+ year old

- Remind your child that they do not have guaranteed privacy in group chats. Conversations can easily be saved or shared, and thoughtless messages can impact their reputation with friends and wider, like professionally.
- If your child is using group chats to get to know new people, discuss strategies they can use to keep themselves safe if they choose to meet (meet in a public space, never go alone, share location).

Glossary

admin	a member of a chat who can perform certain actions such as adding or removing other members.
block	a tool available on many platforms to stop a user from interacting with you.
e2e encryption	(end to end encryption) technology that means messages are only visible to the sender and recipient.
left on read	slang referring to someone reading a message that requires a response, but not sending a reply.
moderator	a member of a chat or community who tries to ensure that others are behaving safely or respectfully.
PM (or DM)	a private message (or direct message) that is sent between two people separate from a group chat.
read receipts	a feature of some apps that allows users to see when a message they have sent has been opened or read.
report	a tool available on many platforms that allows a user to escalate an issue to the platform's safety team, usually because it breaks the terms and conditions or community guidelines.
side chat	a separate chat between two or more members of a larger 'main' chat. Often used to discuss or comment on activity in the 'main' chat.

Appendix 3: 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.