



MONKSEATON HIGH SCHOOL

ICT AND INTERNET ACCEPTABLE USE POLICY

Status:

Statutory policy or document	No
Review frequency	Annually
Approval by	Governing Body
Approval date	11 th October 2023

Publication:

Statutory requirement to publish on school website	No
Agreed to publish on school website	Yes

Review:

Frequency	Next Review Due
Annually	October 2024

1. Introduction and aims

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

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, students, parents/carers and governors.
- 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.
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching students safe and effective internet and ICT use.

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

Breaches of this policy may be dealt with under our staff disciplinary policy / student behavior 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](#)

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 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 facilities, including governors, staff, students, 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.

See appendix 4 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT 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 students, or other members of the school community without the required authorisation.
- 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, homophobic, 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 homework or class assignments, where AI-generated text or imagery is presented as student's own work.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or any other relevant member of staff 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. This must be requested in writing to the Headteacher.

Students may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas where explicitly approved by a member of staff.
- 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.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's behaviour policies / disciplinary procedures.

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

5.1 Access to school ICT facilities and materials

The school's ICT Technician, under the direction of the Business Manager, manages access to the school's ICT facilities and materials for school 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 school'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 the ICT Technician, who will consult with the relevant line manager / Business Manager.

5.1.1 Use of phones and email

Monkseaton High School's email system is an effective tool for supporting the delivery of its services, both internally and externally. As with any other form of written communication care and consideration must be taken in its use, more so than verbal-based communication, as recipients can easily misinterpret language and tone.

Students and staff will be given approved email accounts. All business communication should be undertaken from this account. Users must not use their personal accounts for business use.

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 students 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 ICT Technician and Business Manager immediately and follow our data breach procedure.

Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

Any emails sent by students to external organisations must be authorised by a member of staff before sending.

Staff members are aware that all electronic communication, including emails, should be transparent and open to scrutiny.

Chain letters, spam and all other emails from unknown sources must be deleted without opening.

Spam and threat filtering

The anti-spam monitoring system in place at Monkseaton High School should prevent staff and students from receiving junk mail and offensive or sexually explicit material.

This form of malicious activity is constantly changing and evolving new tactics, and as such from time to time some offensive or explicit material may make it through the anti-spam system.

In such a case, staff members must inform the ICT Technician immediately and in doing so will not be held responsible for the inappropriate content.

Once informed the ICT Technician will inform the Business Manager and advise the Headteacher, who will then manage the incident and report to the appropriate authority as necessary.

Email protection

Staff must comply with the conditions of copyright of any material sent to them or acquired by them via email. Staff must not send email messages which might constitute a legally binding contract without the relevant permission to do so.

Due to the potential for inappropriate use, the sending of global emails is discouraged and Monkseaton High School may also block sending e-mail messages to, or the receipt of them, from certain addresses.

All staff should be aware that anything committed to email can be used in evidence in employment tribunals and formal inquiries, including internal disciplinary, grievance hearings and Freedom of Information requests.

External e-mail

In order to protect the interests of Monkseaton High School, its staff and representatives, the following standard disclaimer is added automatically to all external emails (whether business or non-business related) at the point that they are sent.

This communication is from Monkseaton High School.

The information contained within, and in any attachment(s), is confidential and legally privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of distribution, copying or use of this communication, or the information within, is strictly prohibited and may be unlawful. Equally, you must not disclose all, or part, of its contents to any other person. If you have received this communication in error, please return it immediately to the sender, then delete and destroy any copies of it. Monkseaton High School disclaims any liability for action taken in reliance on the content of this communication.

Staff must not give their personal phone number(s) to parents/carers or students. Staff must use phones provided by the school to conduct all contact with parents / carers, or must withhold their number if calling from a personal device.

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.

The school can record incoming and outgoing phone conversations.

If calls are to be recorded, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.2 Personal use

Staff can use the internet for personal use, preferably outside school hours, as well as break and lunch times, to avoid unnecessary traffic on the network at peak times.

Personal use will be monitored by authorised personnel for access to any inappropriate or explicit sites in the same manner as business use. Whilst we do not actively monitor the sites staff are accessing, there can be no expectation of privacy.

Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices.

Personal use is permitted provided that such use:

- Does not take place during contact time.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no students are present.
- Does not interfere with their job, or prevent other staff or students from using the facilities for work or educational purposes.

Staff may not use the school'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 are also permitted to use their personal devices (such as mobile phones or tablets) in line with the code of conduct.

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 students and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1 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

We allow staff on request to access the school's ICT facilities and materials remotely. They should dial in using a virtual private network (VPN).

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

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

5.4 School social media accounts

The school has an official instagram account, managed by the senior leadership team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

No additional school social media accounts should be created without approval from the Headteacher.

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

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

- Internet sites visited
- Bandwidth usage

- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications.

Only authorised 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.

The Governing Body 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.

With support from the Business Manager, 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 Business Manager, as appropriate.

Any requests by staff for websites to be added or removed from the filtering list must be submitted through an ICT support ticket, and will be checked by the ICT Technician, with approval from the DSL / Business Manager where appropriate.

The school's internet access includes filtering, appropriate to the age and maturity of students.

The ICT Technician ensures that the filtering methods within the school are appropriate, effective and reasonable, with tests performed periodically using the SWGFL test site. Any material that the school believes is illegal is reported to the police. It is the responsibility of all staff to screen for inappropriate content and report this to ICT Technician if this is found.

The combination of the school firewall and content filtering systems are designed to prevent staff and students from accessing or downloading offensive, abusive or sexually explicit material and will block access to certain web sites based upon the inappropriate content.

Due to the increase in the number of websites that contain material of this nature and changing methods of circumventing and bypassing filtering systems, occasional accidental access to such content may occur. In discovering such a case, staff members must inform the ICT Technician and in doing so they would not be held responsible, providing it is reported immediately. If students access or download such material by accident, they must inform a staff member for report to the ICT Technician, and as with staff will not be held responsible provided that they report it immediately.

6. Students

6.1 Access to ICT facilities

Computers and equipment in the school's ICT suites are available to students only under the supervision of staff, with the exception of 6th Form students who are permitted unsupervised access.

Specialist ICT equipment, such as that used for music, or design technology, must also only be used 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 students and confiscate their mobile phones, computers or other devices provided that the authorised staff member has reasonable grounds for suspecting that this:

- Poses a risk to staff or students, 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 students and staff. If the search is not urgent, they will seek advice from the Headteacher / Designated Safeguarding Lead.
- Explain to the student 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 student's co-operation, if the student refuses to co-operate, we will proceed according to our behaviour policy.

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned item. A list of banned items is available in 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 / Headteacher / other member of the senior leadership team 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 student 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 students 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

Any complaints about searching for, or deleting, inappropriate images or files on students' 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 students, in line with the behaviour policy, if a student 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 students, 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.

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) 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 students, and to 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 via email and through our website and social media channels.

7.3 Communicating with parents/carers about student 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 students 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 students 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.

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 students. 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, students, parents/carers and others who use the school'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 school'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 students 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.

The ICT Technician will generate passwords for all new users; these must be changed on first log in by the user. Staff will be given access to passwords generated for students to assist with logging in. Staff are able to reset passwords for students; the ICT Technician can reset passwords for staff.

Users will be forced to change their passwords every 180 days.

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 processed 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 facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT Technician.

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 ICT Technician 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 student 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 ICT Technician.

9. Protection from cyber attacks

Please see the glossary (appendix 4) to help understand cyber security terminology.

The school will:

- Work with Governors, the Business Manager and the IT Technician 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](#)) at least annually, to objectively test that what it has in place is effective.
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe.
 - **Up to date:** with a system in place to monitor when the school needs to update its software.
 - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be.
- Back up critical data daily and store these backups on the Datto backup system, working in conjunction with Synergi.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the ICT Technician.
- Make sure staff:
 - Dial into our network using a virtual private network (VPN) when working from home.
 - Enable multi-factor authentication where they can, on things like school email accounts.
 - Store passwords securely using a password manager.
- Make sure the ICT Technician conducts 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 ICT Technician including, for example, how the school will communicate with everyone if communications go down, who will

be contacted and when, and who will notify [Action Fraud](#) of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)' .

- Work with the Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement.

10. Internet access

The school's wireless internet connection is secure. There are 3 separate Wi-Fi connections. The Staff and Student Wi-Fi is to be used by staff and students and requires a login to use. Visitors is for visitors in school that would not have a login e.g. parents/carers. Internal is for specific devices using a MAC address filter and is configured by the ICT Technician. All Wi-Fi in school is protected by a firewall and monitoring software. Reports are sent to the ICT Technician regularly to ensure that the filtering system is functioning correctly.

If a student or a staff member accesses a site that should be blocked by the firewall, they should report it to the ICT Technician

10.1 Students

Wi-Fi is available throughout the school and is protected by a firewall and monitoring system. School Wi-Fi is to be used on mobile devices provided by the school, such as laptops and iPads. Students may connect personal mobile devices to the Wi-Fi but are only permitted to use it outside or on the ground floor during break and lunch time.

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 / Business Manager or another member of the senior leadership team.

They 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).

11. Monitoring and review

The Headteacher, Business Manager and ICT Technician will monitor the implementation of this policy, ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year along with the online safety policy.

The Governing Body is responsible for reviewing and approving this policy.

12. Related policies

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

- Online safety

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Staff code of conduct
- Data protection
- Mobile phone usage

Appendix 1: Social media cheat sheet for staff

Do not accept friend requests from pupils on social media

10 tips for school staff on Facebook and other social media channels

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be happy showing your students.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there.
8. 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).
9. 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.
10. Consider uninstalling social media apps 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 students).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students 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 student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile.
- Check your privacy settings again, and consider changing your display name or profile picture.
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the student 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.
 - Students 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 student or staff member, our behaviour 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, homophobic, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Appendix 2 : Acceptable use agreement for students

Acceptable use of the school's ICT facilities and internet: agreement for students and parents/carers

Name of student:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose.
- Use them without a member of staff being present, or without a member of staff's permission.
- Use them to break school rules.
- Access any inappropriate websites.
- Access social networking sites (unless a member of staff has expressly allowed this as part of a learning activity).
- Use chat rooms.
- Open any attachments in emails, or follow any links in emails, without first checking with a member of staff.
- Use any inappropriate language when communicating online, including in emails.
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video.
- Share my password with others or log in to the school's network using someone else's details.
- Bully other people.
- Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
 - During assessments, including internal and external assessments, and coursework.
 - To present AI-generated text or imagery as my own work.

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

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (student):

Date:

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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.
- Share confidential information about the school, its students or staff, or other members of the community without relevant authorisation.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote any private business, unless that business is directly related to the school.

I understand 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 ICT Technician know if a student 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 students in my care do so too.

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

Date:

Appendix 4: 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.

TERM	DEFINITION
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.
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.