The Appleton School

ICT and Internet Acceptable Use Policy

Adopted by the Governing Body on	
Signature Chair of Governors	
Next Review Date	

September 2023

Contents

1. Introduction and aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils 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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, 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, pupils, 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 pupils safe and effective internet and ICT use

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

Breaches of this policy may be dealt with under the school's behaviour policy/staff discipline policy/staff code of conduct – which ever are applicable at the time.

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, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 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 pupils, 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 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. Any member of staff that require the use of school ICT facilities (on the school premises and/or remotely) for a purpose that would otherwise be considered an unacceptable use must gain authorisation from the headteacher in advance of use. Students are not permitted to use the school ICT facilities for any unacceptable use.

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

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 policies on behaviour/discipline/staff discipline/staff discipline/staff code of conduct.

Sanctions in place for unacceptable ICT use include:

- Class teacher setting relevant sanction in line with the school behaviour policy
- Appropriate sanctions set by other relevant staff in school
- Revoking permission to use the school's systems

The school's behaviour policy can be found:

https://www.theappletonschool.org/user/pages/08.legal-information/09.policies/Behaviour_Policy_June_2023.pdf

The school's staff code of conduct can be found:
https://www.theappletonschool.org/user/pages/08.legal-information/09.policies/Staff_Code_of_Conduct.pdf

The school's online policy that includes mobile phone and smart technology use can be found:
https://www.theappletonschool.org/user/pages/08.legal-information/09.policies/Online_Safety_Policy.pdf

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

5.1 Access to school ICT facilities and materials

The school's network manager/ICT 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 network manager/ICT manager.

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 pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the SBM/network manager/ICT manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. 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.

The school can record incoming and outgoing phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. Your school's phone system probably has an automated option you can use/adapt.
Explain when you record phone conversations and why. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should speak to the ICT Manager.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Set out your protocol for approving requests here. For instance, you may grant requests to record conversations when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

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 network manager/ICT manager/SBM/headteacher/etc. 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 pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the 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 school's online policy, including the use of mobile phones/personal devices. Staff are to note that the school does have the right to access personal devices if being used on the school site during teaching hours.

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 pupils 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 the information regarding staff/student/parent use of social media in our Communications and Meetings Policy) and use of email (see section 5.1.1 and the relevant sections of the Communications and Meetings Policy, Staff Code of Conduct) 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 Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely. If your school has one, add: They should dial in using a virtual private network (VPN).

Explain the remote access system you use, including:

- Who manages it
- Security arrangements
- Protocols for remote access
- How staff can request 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 as the network manager/ICT manager may require against importing viruses or compromising system security.

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

A copy of the school's data protection policy can be found:
https://www.theappletonschool.org/legal-information/data-protection-policies

5.4 School social media accounts

The school has an official Facebook/Twitter/etc. account, managed by Admin staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The 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 facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- ICT work/documents using the school ICT facilities
- Bandwidth usage
- Email accounts
- Telephone calls
- Staff personal devices if being used for teaching purposes or during the teaching day
- 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 use SMOOTHWALL (IT network manager/DSL and deputies/headteacher) to filter and monitor use of the internet and IMPERO (classroom teacher/IT network manager/DSL) for monitoring work produced using the school ICT facilities. This is outlined in the school's Online Safety policy found on the school website.

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 manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

ICT facilities are available to pupils, at the following times and circumstances:

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL
- Sixth-form pupils can use the computers in the sixth form study area independently, for educational purposes only

6.2 Search and deletion

The headteacher, deputy headteachers and other members of the Senior Leadership Team (including the DSL) are authorised to search, and delete from, an electronic device.

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

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out as highlighted in the school behaviour policy. These items are listed in the school behaviour policy, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / designated safeguarding lead / appropriate member of staff
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, the relevant member(s) of staff 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 pupil was in possession of a banned item. A list of banned items is available in the school's 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 pupil and/or the parent refuses to delete the material themselves

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

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

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS 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(make sure that your searches and confiscation policy reflects the updated DfE guidance, which came into force on 1 September 2022)

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on 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 pupils, 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 section 4.2 and the school's behaviour policy which set out what kinds of sanctions might apply if pupils do any of the above.

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 pupils, 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.

We ask parents/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil 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 pupils 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 pupils 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 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 cybercrime technologies.

Staff, pupils, 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 pupils who disclose account or password information may face disciplinary action.

Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

All staff will use the password manager required by the network manager/ICT manager/SBM/ICT service provider/etc. to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

Staff are required to change their passwords on a regular basis. Pupils are encouraged to do this routinely as well and not to share any changes with other students.

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.

A copy of the school's data protection policy can be found:
https://www.theappletonschool.org/legal-information/data-protection-policies

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 IT manager.

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 IT manager/SBM 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 pupil 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 network manager/SBM/headteacher.

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) 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 (insert frequency – this should be regularly and ideally at least once a day (it can be automatic)] and store these backups on [cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises)
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider/our IT department (if you use an on-premises provider)
- 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 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 [insert frequency – this should be at least annually though ideally every 6 months] and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet connection is secure.

Other information about the school's WiFi includes:

- We use SMOOTHWALL for filtering and monitoring of usage when connected to the school WiFi
- We have generic connections for staff/pupils/parents or carers/the public

We are aware that filters aren't foolproof. If detected, the school will report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the relevant member of staff/service provider.

10.1 Pupils

Pupils are permitted use of WiFi.

- WiFi is available for pupils around the school
- If connected to the Wifi, users are protected by the same SMOOTHWALL filtering and monitoring process when connected to the network.
- Pupils have to access the school WiFi using their individual school password
- The use of WiFi is subject to the same unacceptable/acceptable use as outlined in section 4

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 or as a member of the PTA)
- 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 ICT manager/network manager/SBM/DSL/headteacher. 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 annually.

The governing board is responsible for reviewing and 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
- 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

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards, use a nickname, or use a contraction
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 pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils 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 the social media apps from your phone. The apps recognise WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings - Facebook

- Change the visibility of your posts and photos to **'Friends'**, rather than **'Public'**. Otherwise pupils and their families may be able to see your posts and pictures you've been tagged in, even if you haven't accepted a friend request or they're not on Facebook
- Don't forget to check your old posts and photos – see Facebook's privacy support page for step-by-step instructions on how to do this
- 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
- Prevent search engines from indexing your profile so people can't search for you by name – see Facebook's step-by-step instructions
- **Google your name** to see what information about you is visible to the public
- 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

Check your privacy settings - Instagram

- Change your profile visibility from the default 'Public' setting to 'Private'. Otherwise pupils and their families will be able to see your posts, reels, locations, and who you are following and are followed by. Go to the **Instagram Help Centre** for support with your privacy settings
- If a pupil or parent followed you before you changed your privacy settings, block them to prevent them seeing your posts
- Be careful about giving third-party apps or websites access to your Instagram account, and check app privileges in your phone to see if any apps currently have access. Sharing your information can put your account at risk and make you visible on search engines, even if you have set your account to 'Private'.
- Remember, some information is always public; your username, your bio and your profile picture
- Google your name to see what information about you is visible to the public

Check your privacy settings - Twitter

- If you have a Twitter account specifically for or about teaching, make sure you don't include identifying information about yourself or your school. Use a nickname, for example 'Miss M'
- Change the visibility on your birth date to 'You follow each other' to prevent pupils and parents seeing this personal information. See Twitter's profile visibility guidance for more support
- Remember, your username, biography, location, website and profile picture are always public and can be seen by pupils and parents, even if they don't follow you and you have protected your tweets
- Protect your tweets by checking the box in the 'Audience and tagging' section of your privacy settings. This will mean only your approved followers can see your tweets
- Google your name to see what information about you is visible to the public

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil 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 pupil 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: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for school announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

Signed:

Date:

Appendix 3: Acceptable use agreement for Sixth Form pupils

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

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 teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher 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 teacher
- 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 (pupil):	**Date:**

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

Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for years 7 to 11 pupils

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

Name of pupil:

When I use the school’s ICT facilities (like computers and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren’t wearing all of their clothes
- Share my password with others or log in using someone else’s name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work

I understand that the school will check the websites I visit and how I use the school’s computers and equipment. This is so that they can help keep me safe and make sure I’m following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school’s ICT systems and internet.

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 (pupil):	**Date:**

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

Signed (parent/carer):	**Date:**

Appendix 5: 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 pupils or staff, or other members of the community
- 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 manager know if a pupil 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 pupils in my care do so too.

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

Appendix 6: 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.

Appendix 7: Preparation

- Do not use ICT for the 'sake of it'
- Plan with the ICT resources
- Organise ICT facilities/resources for too many rather than too few lessons
- Plan to use computing specialist terms during the lesson delivery
- Adapt ICT along with subject adaptations
- Decide how best to demonstrate if it will be a necessary part of the lesson
- Plan groups – do not assume every student will have a computer to use as an individual
- Allow enough 'time'
- Always plan and alternative 'non-ICT resourced' lesson

Preparation:

1. DO NOT use ICT for the sake of it – nor simply for reward or motivation – have clear subject specific objectives along with your ICT based expected outcomes.

2. Plan you activities 'with' the software/hardware – do your research and visit the sites, watch the videos you plan to use or want students to access beforehand.

3. Achieving all of your objectives may involve more time than you might expect – time will be spent reminding students of the 'mechanics' – logging in/saving regularly under user area etc. (This should be stated as a matter of fact – never assume all users will do these things automatically). So plan enough time with your ICT resources – a series of lessons. Plan and organise the booking of resources two weeks in advance if possible.

4. Plan to use some computing specialist terms when setting the task – this should not only increase your own working understanding but it will serve to increase the students confidence in you working within this ICT environment, e.g toolbar/copy/window etc.

5. Be aware that a class of students may have very different levels of ICT skills – adapt the ICT context as well as your curriculum-based inputs. Do keep your expectations high – never under value student's previous experience.

6. How will you demonstrate? Showing a past example – or your efforts may be of use as a starter!

- *Whole class – teacher-led talk-through demo? – All eyes on monitors/hands on mouse and keyboard/all ears listening to instructions.*
- *Individual stage by stage set of instructions?*
- *Teacher demonstration to whole class or smaller groups using IMPERO – class also made aware of monitoring of their ICT use/work*

7. Plan the 'groups' of students –

- Individual working?
- Different/similar capabilities ICT/subject knowledge?
- Same/mixed gender groups

* be aware that not all students are happy to share ICT resources
* be aware that some students will be often very willing to provide 'technical support' for others that may be less knowledgeable or skilled. This is not necessarily an issue unless it becomes a prolonged or misinformed or intrusive activity.

8. Plan 'time' generously – leave enough time for saving to user area, spell checking, organising printing, logging off and closing down, returning work station to acceptable standard for next user.

9. Always have an alternative, non-ICT based method of delivery.

Appendix 8: Practical Classroom Management

Remember that you are managing the classroom situation at all times – there may be students in the room with more ICT expertise than you, but this is irrelevant.

1. Students should only ever be in a computer room accompanied by a member of staff. It is useful for them to enter in small groups and in a calm fashion. Coats and bags should be stored away from resources – under desks or pegs where applicable.

2. Where there are desks, students should begin the lesson there. Clear curriculum and ICT objectives explained to the students. The student should manage transition to the ICT resources.

3. Inconsistencies should be reported to ICTtechnicaloffice@theappletonschool.org ASAP.

4. Staff should follow school procedures – including the ICT and Acceptable Use policy. This must include logging on/off and the end of each lesson.

5. Sanctions regarding misuse of either software or hardware should be clearly outlined to students and carried through with if necessary, following this policy and the school's behaviour policy. Incidents should be recorded on SIMS and/or CPOMS if it a safeguarding concern, discriminatory behaviour or bullying concern. Sanctions could include students being restricted from using the school ICT resources. Parents could be asked to pay to cover the costs of any damage to equipment.

6. Students should be encouraged to manage their user areas – organising their files into separate folders, along with deleting files that are no longer required.

7. Students should save to their user areas at regular intervals using Google Drive.

8. Printing should always be a teacher managed activity – students should:

- Ask permission to print
- Have spell checked their work
- Have organised their work in logical/required order
- Only print once

Staff should make themselves familiar with the printer in the room being used and ensure there are sufficient supplies. Staff should ensure they are familiar with how to 'resume' printing that is paused.

9. Staff are required to consistently monitor the students use of the ICT facilities by students in their class using IMPERO. Staff should seek advice from the ICT technical team for advice on using IMPERO. It is a requirement that ALL staff are monitoring the unacceptable use of ICT resources.

Appendix 9: Quick pre-lesson checklist and acceptable use of ICT rooms

1. Are the ICT facilities available?
- booked using the room booking system

2. Do you require ICT support staff at the start/during your lesson?
- this can often be accommodated during your first ICT resourced lesson by liaising with mtitheridge@theappletonschool.org

3. Have you informed your class the lesson is based elsewhere and displayed the Room Change sign outside the original room or will you meet in your timetabled classroom?

4. It is vital that the room is left in state that you would expect to find it!

5. Do not swap/move/unplug hardware without consulting with ICTtechnicaloffice@theappletonschool.org in the first instance.

6. It is a requirement that ALL staff are monitoring the unacceptable use of ICT resources using IMPERO from the staff device in the classroom.

7. Staff must also be monitoring the student's use of the hardware and report any damage immediately.

Appendix 10: Staff guidelines for student use of the ICT resources/internet

A member of staff must supervise **ALL** students **ALL** of the time.

Students and parent/carers must have signed the relevant Acceptable Use Agreements.

Students are expected to respect the ICT facilities.

Students are not permitted to use the internet without the permission from the member of staff present.

Students are not to print directly from the internet and should follow any relevant copyright restrictions.

Students should be made aware about the reliability/validity of information they may find out and to be cautious.

Staff should provide a clear research AIM before they encourage students to search the web – focused and directed use of the resource.

Any inappropriate use of hardware and/or software must be recorded on SIMS/CPOMS as appropriate and as soon as possible.

Any discovery of inappropriate material being produced by students (through IMPERO) must be reported to the DSL and/or Pastoral team immediately and the class teacher to sanction the students in accordance with the school's behaviour policy. Any incidents of discrimination, bullying, child-on-child abuse, extremism/radicalisation must also be reported on CPOMS.

Appendix 11: Meeting digital and technology standards in schools

Filtering and monitoring standards for schools

Standard 1: We will identify and assign roles and responsibilities to manage our filtering and monitoring systems

The importance of meeting the standard
We aim to provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. At the Appleton School the right people are working together and using their professional expertise to make informed decisions.

How to meet the standard
Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
To do this, they will identify and assign:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service providers

We recognise that there is not always capacity for full-time staff for each of these roles and responsibility and therefore, may lie as part of a wider role within the school. However, it will be clear who is responsible and it is possible to make prompt changes to our provision.

Technical requirements to meet the standard
The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders will work closely with governors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will work closely together with IT service providers to meet the needs of our setting. Where appropriate we will ask our filtering or monitoring providers for system specific training and support.

The DSL will take lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

When to meet the standard
The school will regularly review the detail of this information in order to ensure they are meeting this standard.

Standard 2: We review our filtering and monitoring provision annually

The importance of meeting the standard
For filtering and monitoring to be effective it should meet the needs of your pupils and staff, and reflect your specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of our school, we review our filtering and monitoring provision annually.

Additional checks to filtering and monitoring will be informed by the review process so that governing bodies and proprietors have assurance that systems are working effectively and meeting safeguarding obligations.

How to meet the standard
Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review will be recorded for reference and made available to those entitled to inspect that information.

Your IT service provider may be a staff technician or an external service provider.

Technical requirements to meet the standard
A review of filtering and monitoring will be carried out to identify our current provision, any gaps, and the specific needs of our pupils and staff.

We understand:

- the risk profile of our pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what our filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of our pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies we have in place
- what checks are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be done annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

There are templates and advice in the reviewing online safety section of Keeping children safe in education that the school will follow when conducting reviews.

Checks to our filtering provision will be completed and recorded as part of our filtering and monitoring review process. How often the checks take place will be based on our context, the risks highlighted in our filtering and monitoring review, and any other risk assessments. All checks will be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems we will make sure that the system setup has not changed or been deactivated. The checks will include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

We will keep a log of our checks so they can be reviewed. You should record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

We make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before releasing them to staff and pupils
- blocklists are reviewed and they can be modified in line with changes to safeguarding risks

We will use the South West Grid for Learning's (SWGfL) testing tool to check that our filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

When to meet the standard
The school will regularly review the detail of this information in order to ensure they are meeting this standard.

Standard 3: Our filtering system blocks harmful and inappropriate content, without unreasonably impacting teaching and learning

The importance of meeting the standard
We recognise that an active and well managed filtering system is an important part of providing a safe environment for pupils to learn.

We also recognise that no filtering system can be 100% effective. We understand the coverage of our filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet your statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty.

An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

How to meet the standard
Governing bodies and proprietors will support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school.

Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. Where appropriate we will ask our filtering provider for system specific training and support.

Technical requirements to meet the standard
We make sure our filtering provider is:

- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

Where the filtering provision is procured with a broadband service, we make sure it meets the needs of our school.

Our filtering system is operational, up to date and applied to all:

- users, including guest accounts
- school owned devices
- devices using the school broadband connection

Our filtering system:

- filters all internet feeds, including any backup connections

- be age and ability appropriate for the users, and be suitable for educational settings
- handle multilingual web content, images, common misspellings and abbreviations
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provide alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. If our users access content in this way, we will get confirmation from our provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system will be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

Our filtering systems allows us to identify:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked

We conduct our own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

The UK Safer Internet Centre has guidance on establishing appropriate filtering.

Our senior leadership team may decide to enforce Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for our users on top of the filtering service.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Dependencies to the standard
We also check that we meet:

- Broadband internet standards
- Cyber security standards

When to meet the standard
The school will regularly review the detail of this information in order to ensure they are meeting this standard.

Standard 4: You should have effective monitoring strategies that meet the safeguarding needs of your school or college

The importance of meeting the standard
Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Our monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

How to meet the standard
Governing bodies and proprietors support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school.

The designated safeguarding lead (DSL) will take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective. Training should be provided to make sure their knowledge is current. Where required, we will ask our monitoring system provider for system specific training and support.

Technical requirements to meet the standard
Governing bodies support the senior leadership team to review the effectiveness of our monitoring strategies and reporting process. Make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It is made clear to all staff how to deal with these incidents and who should lead on any actions.

The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring.

Device monitoring will be managed by IT staff or third party providers, who need to:

- make sure monitoring systems are working as expected
- provide reporting on pupil device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that your staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts

If mobile or app technologies are used then we will apply a technical monitoring system to the devices, as our filtering system might not pick up mobile or app content.

In the online safety section of Keeping children safe in education there is guidance on the 4 areas of risk that users may experience when online. Our monitoring provision will identify and alert you to behaviours associated with them.

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by pupils
- report any safeguarding concerns to the DSL

The school monitoring procedures are reflected in this policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices.

Where we have a technical monitoring system we will conduct our own data protection impact assessment (DPIA) and review the privacy notices of third party providers. A DPIA template is available from the ICO.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Dependencies to the standard

Check that you meet:

- Cyber security standards

When to meet the standard

The school will regularly review the detail of this information in order to ensure they are meeting this standard.

Appendix 12: Breaches and sanctions

The use of the school’s computer network and Internet connection is a privilege, not a right. Any student user found or believed to be using the service inappropriately, will automatically have their entitlement to use this facility suspended without notice. A student user who violates this policy and breaches his/her agreement may have his or her access to the computer network and Internet terminated indefinitely.

A student user breaches the agreement not only by affirmatively violating the ICT policy, but also by failing to report any violations by other users that come to their attention. Moreover, a student user violates this policy if they permit another student to use their account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school may also take other disciplinary action.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance.

Examples of this level of non-compliance would include:

- Taking food and/or drink into ICT facilities where they are forbidden.
- Sending nuisance (non-offensive) email
- Behaving in a disruptive manner.

Not all first offences will be automatically be categorised at this level since some may be of a significant or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties.

Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12 month period.
- Unauthorised access through the use of another user’s credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libelling another person.
- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded.

Examples of this level of breach would include:

- Repeat moderate breaches.
- Theft, vandalism or wilful damage of/to ICT facilities, services and resources.
- Forging email i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.

- Unauthorised copying, storage or distribution of software.
- Any action, whilst using school computing services and facilities deemed likely to bring the school into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy ICT systems security.
- Attempting to modify, damage or destroy another authorised user's data.
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process – student breaches
An investigation will be carried out, in confidence, by school leadership under the direction of the Headteacher. That investigative report will be passed to the students Head of Year (or Head of Faculty where appropriate), to be considered within the school behaviour policy. Parents will be kept informed of the process and sanctions.

Process – staff breaches
An investigation will be carried out, in confidence, by school leadership under the direction of the Headteacher. That investigative report will be passed to the staff member's Line Manager, to be considered within the school disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.

SANCTIONS:
If students fail to comply with this policy they may have their internet, email and/or computer use restricted for a period of time or withdrawn altogether. Student personal devices, such as mobile phones, maybe confiscated for a period of time or the privilege to bring it into school removed.

Breaking the Student Acceptable Use Policy may lead to:

- Withdrawal of the student's access.
- Close monitoring of the students network activity.
- Investigation of the students past network activity.
- Disciplinary action, including a recommendation for temporary or permanent suspension.
- In some cases, criminal prosecution.

Use of Social Media / Cyber Bullying
The school takes the issue of Cyberbullying and the appropriate use of Social Media very seriously.

Students should not be accessing social media sites unless they have reached the minimum age requirement; such as

- Facebook 13 Years
- Instagram 13 Years
- Twitter 13 Years

If parents allow children to use these and other similar social media sites before they are old enough the school will not take responsibility for resolving issues that may occur.

THE USE OF ICT AND THE LAW
The use of ICT will always leave evidence no matter where the incident occurred; home computer, school computer, and/or mobile phone. The user will leave a 'digital footprint' that can potentially be used to identify them.

Misusing ICT can be a criminal offence under a range of different laws including:

- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- Section 127 of the Communications Act 2003
- Public Order Act 1986
- The Defamation Acts of 1952 and 1996
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Police and Justice Act 2006

For more advice on using ICT safely please visit the following website www.thinkuknow.co.uk