

Acceptable and Responsible Use of Internet Policy

Review date:	Spring 2024
Next review date:	Spring 2025
Person in charge:	Headteacher Mrs. S. Armstrong
Governance:	Safeguarding link governor Mrs. J. Thompson STEM link governor Mrs. G. Clark

Contents

Introduction and aims	
Relevant legislation and guidance	
Definitions	
Unacceptable use	
Sanctions	
Staff (including governors, volunteers and contractors)	
Pupils	
Parents	
Data security	
Protection from cyber attacks	
Internet access	
Monitoring and review	
Related policies	
Appendix 1: Facebook cheat sheet for staff	
Appendix 2: Acceptable use of the internet: agreement for parents and carers	
Appendix 3: Acceptable use agreement for older pupils	
Appendix 4: Acceptable use agreement for younger pupils	
Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors .	
Appendix 6: Cyber security glossary	

Introduction and aims

ICT is an integral part of the way our academy works, and is a critical resource for pupils, staff, volunteers, contractors and visitors. It supports teaching delivery and enhances learning, and provides administrative functions of the academy.

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

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, pupils, parents, volunteers, contractors and visitors;
- Establish clear expectations for the way all members of our community engage with each other online;
- Support the Trust's policy on data protection, online safety and safeguarding;
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems;
- Support the academy in teaching pupils safe and effective internet and ICT use;

Breaches of this policy may be dealt with under the Trust's Code of Conduct & Disciplinary Policy.

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- [The General Data Protection Regulation](#)
- [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](#)
- [The Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2021](#)
- [Searching, screening and confiscation: advice for schools](#)
- [National Cyber Security Centre \(NCSC\)](#)
- [Education and Training \(Welfare of Children Act\) 2021](#)

Definitions

“ICT facilities”: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

“Users”: anyone authorised by the school to use the 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

“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 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.

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary proceedings.

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 (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, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel [i.e. personal or non-encrypted memory sticks]
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data [i.e. using YouTube Converter which may enable inappropriate pop-ups].
- 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 ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data [including personal data] to which a user is not supposed to have access, or without authorisation
- Accessing personal social media platforms using school's ICT.
- 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 mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or

behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Code of Conduct and Disciplinary [available on Every, the school Admin drive or request a paper copy via the Office Manager].

Staff (including governors, volunteers, and contractors)

Access to school ICT facilities and materials

The school's ICT support team [IT Assist/Internal IT] manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, Ipads and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, or who believe they need access to files/facilities for which they do not, should contact the Headteacher, Office Manager and ICT Support Team.

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.

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 and pupils, and must not send any work-related materials using their personal email account. **Staff are advised to use the schools Eduspot/Teacher2parents email/text when contacting parents etc. Staff should not contact parents via Showbie.**

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 sending password protected files, then staff should ring and verify the recipient over the telephone or person when giving the password [do not send the password in another email].**

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 Headteacher and Office Manager immediately and follow our data breach **procedure [record incident on GDPR Sentry]**.

Staff must not give their personal phone numbers to parents 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.

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

Personal use

Staff are not permitted to use school ICT facilities for personal use.

Staff are not permitted to use their personal devices, unless in case of an emergency [such as mobile phones or tablets] and only within the designated areas of the school.

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 could see them.

Staff should take care to follow the school's guidelines on social media and use of email [see section 5.1.1] to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times. School ICT systems should not be used to access personal social media accounts.

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

Remote access

We allow certain staffing roles to access the school's internal network facilities and materials remotely. They should dial in using a virtual private network (VPN).

The VPN is managed by RM. It has a secure connection created using F5 Networks VPN. Protocols for remote access have been selected by RM & maintained by RM. Staff can request remote access through the Headteacher.

We also allow staff to work on documents remotely using our MS TEAMS account. This is managed by IT Assist or NLLT central team.

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 **i.e. using work devices only for viewing and not personal devices**. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the Headteacher and ICT support team may require from time to time 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.

Please refer to the NLLT Data Protection Policy located on EVERY and the school Admin drive or ask the Office Manager for a paper copy.

School social media accounts

The school has an official Facebook page, managed by The Deputy Headteacher and Office Manager. 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 can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage [network capacity]
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may 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

Pupils

Access to ICT facilities equipment and facilities available to children:

- Pupils will be provided with an account linked to the school's online learning platforms, which they can access from any school device by using the Ipad application or desktop short cut.
- Pupils will have access to class PC computers and Ipad devices with approved programmes suitable to age.
- Main class teaching computers and equipment are only to be used by pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, coding or design and technology, must only be used under the supervision of staff.

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's [guidance on searching, screening and confiscation](#), the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour; Suspension and Exclusion policies, 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 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 and 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 ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data [including personal data] to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Parents

Access to ICT facilities and materials

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

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

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 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 to sign the agreement in appendix 2.

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee

security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

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

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password generator/allocated passwords generated by the programme/application and keep these in a secure location in case pupils lose or forget their passwords.

Individual pupil Ipads will have a generic password to enable pupils to share devices across the school. Pupil individual passwords must not be saved in individual devices and personal work should be saved to Showbie.

Regular wiping/clearing of devices to be completed to reduce the risk of data breaches.

Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and antivirus products will 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.

Data protection

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

The NLLT data protection policy may be located via EVERY, the school Admin drive or a printed copy may be requested via the school's Office Manager.

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 school's ICT support team under agreement from the Headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher 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 closed down completely at the end of each working day.

Encryption

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

School staff may only use work devices [including computers and encrypted 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.

Protection from cyber attacks

Please see the glossary [appendix 6] to help you understand cyber security terminology.

The school will:

- Work with governors, Computing Lead and school's ICT support team to make sure cyber security is given the time and resources it needs to make the school secure.
- Provide regular 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 [this one](#)) to objectively test that what it has in place is up to scratch
 - 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 up to scratch and secure as they can be

Back up critical data

ALL FILES ARE BACKED UP EVERY NIGHT TO ONSIGHT BACKUP & OFFSITE BACKUP. ALL SERVER OPERATING SYSTEMS ARE BACKED UP EVERY SUNDAY NIGHT 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) Scholarpack to our cloud-based provider.

Make sure staff:

- Dial into our network using a virtual private network (VPN) when working from home/log onto their MS TEAMS account
- 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 seeing if they have the [Cyber Essentials](#) certification.

Develop, review and test an incident response plan with the Trust and ICT support team, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed 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.

Internet access

The academy internet connection is secured and managed through the academy's ICT Support Team [IT Assist]. All access to the internet through the academy network, including through domain-controlled devices and user devices connected to the academy's Wi-Fi network are subject to filtering. This service is provided by RM and works to filter the latest risks and threats, additional risks to safeguarding or academic progress can be restricted by the academy's ICT Support Team with the permission of the Headteacher, ensuring that the academy is taking all reasonable precautions to ensure that users access only appropriate material. In addition the school has a monitoring system called SENSO. Filtering and monitoring strategies are selected by the academy, in discussion with the provider where appropriate. The filtering strategy will be suited the age and curriculum requirements of the pupils.

However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on an academy computer. Neither the academy nor RM can accept liability for the material accessed, or any consequences of Internet access.

If staff or pupils discover unsuitable sites, the URL [address] and content must be reported to the Internet Service Provider via the Headteacher/Academy ICT support and parents will be informed. The academy's ICT support team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

If a member of staff or student is able to access a website which they feel should be filtered and is inappropriate for academy, this should be reported immediately to the Headteacher and this should be raised with the academy's ICT support team.

Separate wifi access codes have been created for approved access on site with differing levels of filtering suitable to access e.g. Staff, Pupil, Visitor/Guest. A small number of visitor/guest accounts are available which are tracked and monitored. Access will only be for specific approved reasons i.e. training hosted on site. Personal devices must to be used to access either the Staff or Pupil wifi.

Monitoring and review

The headteacher and Local Governing Body 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 annual by the Headteacher and Local Governing Body.

The Local Governing Body is responsible for approving this policy.

Related policies

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

- Child protection
- Behaviour
- Staff discipline
- Data protection
- Anti-bullying

Don't accept friend requests from pupils on social media

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 not, ensure 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 just as 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 Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils 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 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. 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.

What to do if... A parent adds you on social media


- It is at your discretion whether to respond. Bear in mind that:
 - Responding to one parent'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'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 know that you're doing so.

What to do if... 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 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

<u>Acceptable use of the internet – agreement for parents and carers</u>	
	
Name of parent/carer:	
Name of child:	
<p>Online channels are an important way for parents/carers to communicate with, or about, our school.</p> <p>The school uses the following channels:</p> <ul style="list-style-type: none"> • school website • our official Facebook page • school email • school text (for school announcements and information) • online learning platforms e.g. Showbie and MS TEAMS <p>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).</p> <p>When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:</p> <ul style="list-style-type: none"> • 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 <p>I will not:</p> <p>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 if they aren’t 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.</p> <p>I will contact the school and speak to the appropriate member of staff [i.e. the class teacher in the first instance] if I’m aware of a specific behaviour issue or incident.</p> <p>I will not upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children’s parents/carers.</p>	
Signed:	Date:

Appendix 2: Acceptable use of the internet – agreement for pupils

Acceptable use of the internet – agreement for pupils



Name of pupil:

When I use the school's ICT facilities (like IPADS and computers) and internet in school:

- I will ask permission before using the Internet
- I will use my own login and passwords
- I will only look at or delete my own files
- I will ask for permission before taking or sending photographs of someone else
- I understand that I must not bring my own device into school [including SMART watches]
- I will only email people my teacher has approved for learning purposes
- I will ask for permission before opening an email or an email attachment sent by someone I do not know
- The messages I send will be polite and sensible
- I understand that I must not give my home address or phone number, or arrange to meet someone I do not know
- I will not use Internet chat
- I will not use the Internet for playing games that I haven't been given permission to go on
- If I see anything I am unhappy with or if I receive messages I do not like, I will tell the teacher or a TRUSTED ADULT immediately
- I understand that the school may check my computer files and the Internet sites I visit
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers and my parents will be informed

Signed (pupil):

Date:

Parent/carer agreement:

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 2: Acceptable use of the internet – agreement for staff, governors and volunteers

Acceptable use of the internet – agreement for staff, governors and volunteers



Name of staff member/governors/volunteer:

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 private businesses, 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 support team [IT Assist] 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:

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.
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.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like 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	Programs 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 executives.