Taverham High School
An 11-18 Academy
Inspire | Empower | Achieve

ICT and Internet Acceptable Use Policy

Trustees	Board of Trustees
Staff	DHY
Review Due	Spring 2025
Ratified by Trustees	Spring 2023

Contents

1. Introduction and aims 2

2. Relevant legislation and guidance 3

3. Definitions 3

4. Unacceptable use 4

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

6. Pupils..10

7. Data Security..11

8. Protection from cyber attacks..13

9. Monitoring and review 14

10. Related policies.. 14

Appendix 1: Acceptable use agreement for staff, trustees, volunteers and visitors 15

Appendix 2; Acceptable Use Agreement for Pupils..16

Appendix 3: Glossary of cyber security terminology..17

1. Introduction and aims

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

However, the ICT resources and facilities our school uses 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 and trustees
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption 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 trustees, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our:

- Disciplinary procedure
- Staff code of conduct
- Discipline guidelines on conduct for employees

2. 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

3. 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 trustees, 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 3 for a glossary of cyber security terminology

4. 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 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
- 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
- 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
- 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
- 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.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's or ICT Manager's discretion.

4.2 Sanctions

Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on:

- Disciplinary procedure
- Staff code of conduct
- Discipline guidelines on conduct for employees

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

5.1 Access to school ICT facilities and materials

The school's ICT manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets 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, should contact the ICT manager.

Requests should be put in writing to the 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 accounts.

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 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.

Always double-check that the email has been addressed to the correct recipient(s).

It is essential that any data entered into the subject field of any email does not contain personal data.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer (MEG) immediately and follow our data breach procedure.

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. If staff do use their phone in exceptional circumstances then staff members must withhold their phone number.

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.

To comply with GDPR regulations emails will not be kept for any longer than 2 years. All emails, in any location in your mailbox, will automatically go into an archive folder after 30 months and will be permanently deleted after 3 years.

The school has a ‘Communication Guidance for Staff’ document which can be located in Teams > Staffroom > Staff Wellbeing or here

5.2. Internet access

The school uses enterprise grade technology to provide web filtering and Internet security. All website traffic is recorded and can be monitored. The solution in place meets all the functionality set out by guidance released by the Department for Education. Although extremely robust, the system is not foolproof. If you are worried about anything you or a child saw online, please report it immediately to the IT Manager.

The school has a secure guest wireless network to accommodate bring your own device (BYOD). This is available in the Pavilion, Library, Canteen, 6th Form, Student Support and SLT corridor. A guest wireless network guide is available from Reception and 6th Form. When using the guest network, users are subject to the same level of filtering applied to school computers. Students and staff are required to adhere to the same ICT acceptable use policy. All browsing and web traffic is recorded. Students and staff authenticate with their school username and password.

If you use filtering, be aware that filters aren’t foolproof. If you are able to access an inappropriate site or a site has been filtered in error, please contact ICT support.

5.3 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The ICT manager/headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no 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.

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 (see section 5.5) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.4 Remote access

Public Wi-Fi is available just about everywhere, but it also poses security risks to the personal information available on our laptops and smartphones.

There are two kinds of public Wi-Fi networks: secured and unsecured.

An unsecured network can be connected to without any type of security feature like a password or login. Data transmitted is unencrypted (i.e.as plain text) may be intercepted and read by hackers with the correct knowledge and equipment. This includes data from any services which require a login protocol.

A secured network requires a user to agree to legal terms, register an account, or type in a password before connecting to the network. Data transmitted is encrypted and cannot be intercepted.

We do not advise accessing School ICT facilities on an unsecured network.

If you choose to access School ICT facilities on a personal device, you must ensure the device is secured with either a complex password, PIN or biometric print. It is important to make sure you keep your device up to date by applying the latest security and firmware updates. Where possible, ensure you have anti-virus software and make sure this is kept up to date. Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care, in accordance with our data protection policy and other school policies.

Only devices that have been issued and configured by the school can be used to remotely access the school's internal network, for example shared files or personal documents. The system used is a secure virtual private network (VPN) which is managed by the IT Department. Trying to use alternate methods to gain access is not permitted. Staff that have a requirement to operate remotely to access the school's internal network will be trained by the IT Department on how to use the software.

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.

Our Data Protection Policy can be located on Teams under policies > statutory

5.5 School social media accounts

Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Myspace, Flickr and YouTube.

Roles, responsibilities and procedure

Staff should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media;
- ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the school;
- be aware that any excessive use of social media in school may result in disciplinary action;
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, or even future employers, to read. If in doubt, don't post it!

Acceptable use

Staff should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, staff using social media should conduct themselves with professionalism and respect.

Staff should not upload any content on to social media sites that:

- is confidential to Taverham High School or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings Taverham High School into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

Staff should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook and Twitter. All communication with parents via social media should be through Taverham High School's social media accounts. Staff should note that the use of social media accounts during lesson time is not permitted.

Safeguarding of pupils and employees is the responsibility of all employees and this should also be taken into consideration when using personal social media sites inside and outside of the school. Employees should not link their own personal social media sites to anything related to the school, this includes, but is not limited to; adding school logos or the use of text which imitate Taverham High School.

Where a member of staff is related to a pupil the school should be made aware, if they are not already, and consideration given to whether any safeguards need to be put in place. Employees are advised not to use or access the social media sites of pupils, without due reason e.g. safeguarding purposes, however, this may not be possible if the pupil is a relation of or to the employee.

Staff are not permitted to set up, control or modify social media accounts linked to Taverham High School unless permission has been granted by the Senior Leadership Team.

All social media enquires should be directed to Arlene Warwick to ensure protocols are met and are in line with school policies.

5.6 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
- 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.

Under data protection law this type of monitoring is called 'occasional monitoring'. This is where the employer introduces monitoring as a short-term measure to address a particular issue e.g. performance or conduct where concerns are of the nature explained above. Where monitoring takes place, schools must have due regard to article 8 of the European Convention on Human Rights, which means the employee still has a right to privacy in the workplace. A formal or informal impact assessment will be carried out prior to any monitoring to ensure the monitoring conducted is reasonable and proportionate to the issue that it will address.

6. Pupils

6.1 Access to ICT facilities

- ✓ "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 www.taverhamhigh.norfolk.sch.uk/home/portals
- ✓ "Sixth-form pupils can use the computers in the sixth form study centre and common room independently for educational purposes only"

6.2 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.

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 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

7. 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.

7.1 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 who disclose account or password information may face disciplinary action.

Creating Passwords using Passphrases

Using passphrases is a good way of constructing strong passwords and helps with remembering them. Passwords constructed in this way, will typically consist of letter, numbers and special characters which are used to represent the words or meaning of a phrase. The following example describes this process:

Example:

Step 1 – Choose a phrase – For example: 'I catch the number 14 bus on Fridays'

Step 2 – Use the first character of each word: I c t n 14 b o f

Step 3 – Mix with lower and uppercase letters: iCTn14bOf

Step 4 – Incorporate special characters (such as !@#$%%^&*()_+) and numbers to increase the complexity. Using this method, the final password could be:

I*CTn#14bOf5

Incorporate special characters and numbers into your password is a way which helps you to remember where they should be e.g. could be after every 2nd, 4th, or 5th letter – or similar 'system' which is meaningful to you.

The more letters, special characters and numbers used and the longer the password containing these is, the stronger the password will be.

7.2 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 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.

7.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school’s data protection policy. Inappropriate access or disclosure of employee data constitutes a data breach and should be reported immediately in accordance to the school’s data protection policy. It may also constitute a disciplinary offence, which will be dealt with under the school’s disciplinary procedure.

Employees should not copy and paste any images or text from or make links to images on other sites on the internet unless the other site specifically says that the images and/or text have been copyright cleared for use in that purpose.

Consideration should be given to what is being posted with regards to:

- is the information being posted in the public domain?
- has permission been granted to publicise it from the person who created it?
- is the person who created it aware that the material is going to be made available on the internet?

Our Data Protection Policy can be located on Teams under policies > statutory

7.4 Access to facilities and materials

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

These access rights are managed by the ICT Manager and Data 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 ICT Manager 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.**

7.5 Encryption

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

Where there is a requirement to store data on removable media (e.g. USB stick), devices must be encrypted, and a copy of the data must be stored elsewhere (e.g. School file store) to protect against loss or damage. For help encrypting removable devices, please see ICT Services.

8. Protection from cyber attacks

Please see the glossary (appendix 3) to help you understand cyber security terminology.

The school will:

- ✓ Work with trustees and the ICT 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; Cyber Essentials, annually, 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 daily and store these backups on the cloud and on-site using Network Attached Storage.
- ✓ Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based 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 seeing if they have the Cyber Essentials certification
- ✓ Develop, review and test an incident response plan with the IT department, 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 tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

✓ Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Process to follow if a user account is suspected of being compromised:

If it is suspected that a user account has been compromised, whether through negligence or malicious intent from internal or external sources the steps below need to be followed to ensure that no further information or accounts are compromised.

1. Disable the account in question on the Taverham High School Network, Office 365 and Azure Active Directory.
2. Sign the account out of all active sessions using the Azure Active Directory Portal
3. Choose a secure password using the method mentioned in the 'Creating Passwords using Passphrase's' guide in this policy
4. Isolate and perform security scans on the main school devices that the account has used and apply any missing security updates however these are set apply automatically
5. Investigate any suspicious activity on the account, check login locations, perform mail flow check
6. Inform the user of the compromised account and re-issue a copy of the ICT policy and issue password reset for next logon attempt
7. Report any findings to Data Protection Officer
8. Continue to monitor the account for any suspicious activity

9. Monitoring and review

The headteacher, SLT Lead and ICT Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy relies on employees acting responsibly and in accordance with the outlined restrictions. Where employees have concerns that a colleague is acting in breach of the outlined restrictions they should raise this with the Headteacher or Chair of Trustees if the concerns relate to the Headteacher.

If the concern involves possible inappropriate interaction between a colleague and a pupil, referral should be made to the Headteacher, unless the concern is about the Headteacher, when it should be reported to the Chair of Trustees.

This policy will be reviewed every 2 years.

The board of trustees is responsible for approving this policy.

10. Related policies

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

- Safeguarding and child protection
- Data protection
- Disciplinary procedure
- Staff code of conduct
- Discipline guidelines on conduct for employees
- Remote Learning
- Behaviour Policy

Appendix 1: Acceptable use agreement for staff, trustees, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff and trustees.

Name of staff member/trustee:

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 confirm that I have read the school's ICT policy in full.

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/trustee):	**Date:**

Appendix 2: Acceptable use agreement for 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
- Share my password with others or log in to the school’s network using someone else’s details
- Bully other people

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 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 3: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
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
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.