To inspire, enrich and nurture so each individual reaches their full potential

Hatfield Community Free School, Briars Lane, Hatfield, Herts, AL10 8ES
Website: www.hcfs.org.uk **Telephone:** 01707 276018 **Email:** office@hcfs.org.uk

@hatfieldcfs1 @hatfieldcfs

Principal: Mrs Victoria Hobson

The HCFS is a company limited by Guarantee Registration number 07648654

ICT Acceptable User Policy

April 2024

To be reviewed biennially in the Summer Term

Next Review: April 2026

History of Document

Issue No.	Date Issued	Prepared By	Approved By	Comments
Issue 1	Jan 2022	Jane Sutton	Victoria Hobson	Policy reviewed and updated in line with model from The Key
Issue 2	April 2024	Victoria Hobson	Victoria Hobson	

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), 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, parents 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.

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
- 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: 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 agreed by an authorised users.

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 Six 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 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;
- 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;
- 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 Principal 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 (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 Principal's discretion.

4.2 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 behaviour/discipline/staff discipline /etc.

School's Behaviour Policy and Code of conduct for Parents, Carers and visitors can be found on the school's website.

5. Staff (including trustees, volunteers and contractors)

5.1 Access to school ICT facilities and materials

The Principal's PA, works with Herts for Learning to manage 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 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 Principal. Access to files/folders is at the discretion of the Principal.

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 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 Principal and the SBM immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. 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.

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

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

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

5.2 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 Principal 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 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 should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.3 Remote access

We allow staff to access the school's network remotely. The Principals PA, in conjunction with Herts for Learning, will advise on access and set up on a school device for members of staff who require it.

Staff accessing the HCFS network 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 take such precautions against importing viruses or compromising system security.

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

The school's GDPR Data Protection Policy can be found on the school's website – www.hcfs.org.uk

5.4 School social media accounts

The school has an official Facebook and Instagram Account, managed by the Senior Leadership Team and the 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.

5.5 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.

Our Trust 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 as appropriate.

6. Pupils

6.1 Access to ICT facilities

The following are available for use by Pupils/Staff

- Laptops/Chromebooks/I Pads are available to pupils only under the supervision of staff;
- Pupils will be provided with login details to the school's online platforms.

6.2 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.

7. Parents

7.1 Access to ICT facilities

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) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Principal's discretion.

Where parents 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 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.

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

All staff will keep their passwords secure. Passwords for the pupil's online accounts will be generated by the Computing custodian in collaboration with the Herts for Learning technician.

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 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 network.

No personal devices will be allowed access to the school's network apart from a member of staff's mobile phone, which will be allowed to have access to HCFS Guest Wi-Fi.

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.

The GDPR Data Protection Policy can be found on the school's website – www.hcfs.org.uk

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 Principal.

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 Principal 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.

8.5 Equipment security

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

School staff may only use equipment supplied by the school to access school data, work remotely, or take personal data (such as pupil information) out of school.

Use of such personal devices will only be authorised by the Principal. Staff must provide details of security/encryption on the personal device.

9. Protection from cyber attacks

Please see the glossary (Appendix Six) to help you understand cyber security terminology.

The school will:

- Work with Trustees and Herts for Learning who help manage the school network 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 (Herts for Learning) 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 is routinely time tabled overnight and these backups are stored on a cloud based program and on a hard drive that is stored within school;
- Make sure staff:
    - Only access the school's network via a school provided device, which has been setup by the Herts for Learning technician;

- The Principal will 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;
- Develop, review and test an incident response plan with Herts for Learning for example, including how the school will communicate with everyone if communications go down. This will be reviewed and tested annually.

10. Internet access

The school wireless internet connection is secured.

School's Wi Fi arrangements are as follow:

- Internet filtering is maintained by Herts for Learning and RM Education the school's broadband supplier;
- All staff and pupils have the same settings for Internet Filtering within school which is managed by Group Policy;
- The school has a Guest Wi Fi connection for visitors to school;
- Filters aren't fool-proof and if an inappropriate website is found it should be reported to the Principal.

10.1 Pupils

All the school's Laptops/Chromebooks/iPads connect to the school's Wi-Fi:

- Pupils are not allowed to bring into school personal devices;
- Mobile phones are held in a secure location from the start of the day till the end.

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless granted by the Principal.

The Principal will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer);
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or audit purposes.

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Principal and School Business Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

Appendix One – Facebook

10 rules for school staff on facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your 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

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

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 Two – 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: • Emails from the school's office account and arbor; • Tapestry (for EYFS only).
When communicating with the school via official communication channels, 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 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. 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 other children's parents/carers

Signed:	Date:

Appendix Three – Acceptable use agreement for younger pupils

Name of child:
When I use the school's ICT facilities (laptops/Chromebooks/ I Pads) and get 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 Four – Acceptable use agreement for older pupils

Name of child:

When I use the school's ICT facilities (laptops/Chromebooks/ I Pads) and get on 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 Five – Acceptable use agreement for staff, trustees, volunteers and visitors

Name of staff member/trustee/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 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) 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 Six – Glossary of cyber security terminology

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

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
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.