

ACCEPTABLE USE POLICY

This section should be completed following ratification of the Policy.

| | |
|------------------------|---|
| Audience | All school staff, Trustees, Members, parents and school community |
| Ratified | Oct 2024 |
| Other Related Policies | Whistleblowing Policy, Online Safety Policy, Code of Conduct & Safeguarding & Child Protection Policy |
| Policy Owner | Trust Safeguarding Team, ARC Committee |
| Review Frequency | Within 18 months |

Ownership

Preston Hedges Trust is responsible for the production and maintenance of this document. It is issued by the clerk, clerk@prestonhedges.org to whom any change requests or queries should be directed.

Contents:

| Page | Content |
|------|---|
| 3 | Statement of Intent |
| 3 | Legislation and Guidance |
| 4 | Definitions |
| 4 | Unacceptable Use |
| 6 | Staff (Including Trustees, Volunteers and Contractors) |
| 9 | Pupils |
| 10 | Parents |
| 10 | Data Security |
| 12 | Protection from Cyber Attacks |
| 13 | Internet Access |
| 14 | Appendix 1: Facebook Cheat Sheet for Staff |
| 16 | Appendix 2: Acceptable Use Agreement (<i>staff, governors, volunteers and visitors</i>) |
| 17 | Appendix 3: Acceptable Use Agreement (EYFS) |
| 19 | Appendix 4: Acceptable Use Agreement (KS1) |
| 21 | Appendix 5: Acceptable Use Agreement (KS2) |
| 25 | Appendix 6: Glossary of Cyber Security Terminology |

1. Statement of Intent

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

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

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the Trust and school community engage with each other online
- Support the Trusts policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the Trust or schools through the misuse, or attempted misuse, of ICT systems
- Support the schools 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 staff code of conduct, disciplinary policy and behaviour policy.

2. Legislation and guidance

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

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2023](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

- [Meeting digital and technology standards in schools and colleges](#)

3. Definitions

- ICT facilities: all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- Users: anyone authorised by the Trust or school to use the Trust's / school's 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 user
- Authorised personnel: employees authorised by the Trust / school to perform systems administration and/or monitoring of the ICT facilities
- Materials: files and data created using the Trust's/ school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- Parents: References to Parent, in relation to a child or young person, includes any person who is not a parent but who has parental responsibility, or has care of the child.

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the Trust's / school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust's / school's ICT facilities includes:

- Using the Trust's / school's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's /school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's /school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the Trust, school, its pupils, or other members of the school community

- Connecting any device to the Trust's /school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust's /school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the Trust's /school's ICT facilities
- Removing, deleting or disposing of the Trust's /school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust /school
- Using websites or mechanisms to bypass the Trust's /school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
 - 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 Trust / school reserves the right to amend this list at any time. The Principal / COO will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's / school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Trust / 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 / COO's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust's policies on behaviour / discipline / staff code of conduct.

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

5.1 Access to Trust / school ICT facilities and materials

The Trust's IT Service Provider (Sweethaven) manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Trust's IT Service Provider (helpdesk@sweethaven.co.uk)

5.1.1 Use of phones and email

The Trust provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

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

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

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

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

If staff send an email in error that contains the personal information of another person, they must inform the Principal or COO immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils.
School phones must not be used for personal matters.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. Principals or other members of the Executive Team may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time
- 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 (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone, while children are present. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time for personal reasons. For instance (this list is non-exhaustive):

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The Principal will decide on a case-by-basis whether to allow for special arrangements.
If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

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

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

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

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions 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, which can be found on the schools website.

5.4 School social media accounts

The school has an official Facebook, Twitter and Instagram accounts, managed by the Principal and the Marketing and Communications Officer. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

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

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

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

The trust monitors ICT use in order to:

- Obtain information related to trust business

- Investigate compliance with trust policies, procedures and standards
- Ensure effective trust 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

Filtering and monitoring, compliant with the requirements of Keeping Children Safe in Education 2024 DfE Statutory guidance is in operation within the Trust. The reports generated as a result of filtering and monitoring activities are only accessible to authorised users.

6. Pupils

6.1 Access to ICT facilities

ICT equipment, such as laptops, tablets and VR headsets are available to pupils only under the supervision of staff

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 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 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 or 'Friends') 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.

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 and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features

- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 Data protection

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

8.4 Access to facilities and materials

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

These access rights are managed by the Principal or COO.

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 or COO immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

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

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Principal.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.
The school will:

- Work with ARC Committee and the IT service provider 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 Trust will verify this by annually auditing that what it has in place is effective
 - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
 - Up to date: with a system in place to monitor when the school needs to update its software
 - Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be
- Back up critical data and store these backups on cloud based backup systems and external hard drives that aren't connected to the school network
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based service 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 the Principals / COO work with the IT service provider to conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#) certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually.

10. Internet access

The school's wireless internet connection is secure.

- Use of Smoothwall filtering in line with Internet Watch Foundation guidelines.
- Use separate connections for staff/pupils and guests

10.1 Pupils

Pupils access the trust's Wi-Fi when using trust devices. Pupils access these using a their own log or other trust subscribed programs. The Wi-Fi password is set on student devices through server policy, so the wireless key is never known to students.

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is 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 or as a member of the PTA/'Friends')
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

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

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

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/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
 - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

- When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 that 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
- Take photographs of pupils without checking with teachers first
- 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 will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree 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 that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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

Date:

Appendix 3: Acceptable Use Agreement (EYFS)

| | |
|---|---|
| <p>My Learning</p>  | <ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. |
| <p>My Online Safety</p>  | <ul style="list-style-type: none"> • I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen. |
| <p>Using the Internet at School</p>  | <ul style="list-style-type: none"> • I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake. |
| <p>Using the Internet at Home</p>  | <ul style="list-style-type: none"> • I will tell a trusted adult if I see something that upsets me on the screen |

I understand that these rules help me to stay safe and I agree to follow them. I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

My Name is _____

Parents / Carers: I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.





I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parents Signature_____ Date_____

Appendix 4: Acceptable Use Agreement (KS1)

| | |
|---|--|
| <p>My Learning</p>  | <ul style="list-style-type: none"> • I will use school devices (laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. |
| <p>My Online Safety</p>  | <ul style="list-style-type: none"> • I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen. |
| <p>Using the Internet at School</p>  | <ul style="list-style-type: none"> • I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake. |
| <p>Using the Internet at Home</p>  | <ul style="list-style-type: none"> • I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • Where I have my own username and password, I will keep it safe and secret. • I will tell a trusted adult if I see something that upsets me on the screen. <p>My use of Social Media and Gaming</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. |

| | |
|--|---|
| | <ul style="list-style-type: none"> I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying. |
|--|---|

I understand that these rules help me to stay safe and I agree to follow them. I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

My Name is _____

Parents / Carers: I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.



I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.


I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parents Signature _____ Date _____

Appendix 5: Acceptable Use Agreement (KS2)

| | |
|---|--|
| <p>My Learning</p>  | <ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it. |
| <p>Using the Internet at School</p>  | <ul style="list-style-type: none"> • I will only visit sites that are appropriate to my learning at the time <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my username and password safe and secure - I will not share it. I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may steal it. <p>My role as a Digital Citizen.</p> <ul style="list-style-type: none"> • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. |

| | |
|---|--|
| | <ul style="list-style-type: none"> • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission. |
| <p>Using the Internet at Home</p>  | <ul style="list-style-type: none"> • I will ask permission and only use the devices, apps, sites and games I am allowed to and when I am allowed to • I will be a good friend online – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them. • I will not bully other – I know just calling something fun or banter doesn't stop it maybe hurting someone else. I will not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell a trusted adults. • I will be careful what I click on and not click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so I will always check. • I will ask for help if I am scared or worried and talk to a trusted adult if anything upsets me or worries me on an app, site or game. • I will tell a trusted adult if I see or someone send me something bad – I know it's not my fault and I won't get in trouble, but I will not share it. • I will only communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about. • I know online friends might not be who they say they are – I will be careful when someone wants to be my friend. Unless I have met them face to face, I know I can't be sure who they are. • I will never pretend to be someone else online – it can be upsetting or even dangerous. |

| | |
|--|--|
| | <ul style="list-style-type: none"> • I will check with a parent/carer before I meet an online friend the first time; I will never go alone. • I will not go live (videos anyone can see) on my own – and always check if it is allowed. I will check with a trusted adult before I video chat with anybody for the first time. • I will not take photos or videos of people without them knowing or agreeing to it – and I will never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe. • I will keep my body to myself online and will never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I will not send any photos or videos without checking with a trusted adult. • I will not do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I will say no, stop chatting and tell a trusted adult immediately. • I will follow all age rules and only register for sites or apps that are suitable for my age • I will be private online and only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again. |
|--|--|

I understand that these rules help me to stay safe and I agree to follow them. I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

My Name is_____

Parents / Carers: I understand that the school has discussed the Acceptable Use Agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parents Signature_____ 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](#).

| 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 (such as bank details) or encouraging them to visit a fake website. |
| Ransomware | Malicious software that stops you from using your data or systems until you make a payment. |
| Social engineering | Manipulating people into giving information or carrying out specific actions that an attacker can use. |
| Spear-phishing | A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts. |
| Trojan | A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer. |
| Two-factor/multi-factor authentication | Using 2 or more different components to verify a user's identity. |

| Virus | Programmes designed to self-replicate and infect legitimate software programs or systems. |
|-------------------------------|---|
| Virtual private network (VPN) | An encrypted network which allows remote users to connect securely. |
| Whaling | Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation. |