



Hebden Royd C.E. (VA) Primary &
Nursery School

ICT & Acceptable Use Policy 2024

Approved by:

Headteacher &
Governing Body

Date: January 2023

Last reviewed on:

February 2024

Next review due by:

February 2025

Contents

1. Introduction and aims	2
2. Relevant legislation and guidance.....	3
3. Definitions.....	3
4. Unacceptable use.....	3
5. Staff (including governors, volunteers, and contractors)	4
6. Pupils	6
7. Parents.....	7
8. Data security	8
9. Protection from cyber attacks.....	9
10. Internet access	10
11. Monitoring and review	10
12. Related policies	10
Appendix 1: Facebook cheat sheet for staff.....	11
Appendix 2: Acceptable use of the internet: agreement for parents and carers	13
Appendix 3: Acceptable use agreement for Key Stage 2 pupils	14
Appendix 4: Acceptable use agreement for Key Stage 1 pupils	15
Appendix 5: Acceptable use agreement for EYFS pupils	16
Appendix 6: Acceptable use agreement for staff	17
Appendix 6: Acceptable use of the school's ICT facilities and the internet: agreement for governors, volunteers and visitors	198
Appendix 7: Glossary of cyber security terminology	19

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), governors, 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 governors
- 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 governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct.

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

See appendix 6 for a glossary of cyber security terminology.

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

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 (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

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/staff code of conduct

Please see the school website for these policies.

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

5.1 Access to school ICT facilities and materials

The school's network manager (Calderdale IT Services) 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 headteacher.

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.

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

Staff should not share their personal email addresses with parents and pupils, and should not send any work-related materials using their personal email account unless in extreme.

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 headteacher 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.

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. Personal use of ICT facilities must not be overused or abused. The 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 constitute 'unacceptable use', as defined in section 4
- › 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) so long as it does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

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 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 ensure 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. They should dial in using a virtual private network (VPN). For details of access, see the school administrator.

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 take such precautions as Calderdale IT Support Team may require from time to time against importing viruses or compromising system security.

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

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

6. Pupils

6.1 Access to ICT facilities

- › Computers and equipment 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 may be provided with an account linked to the school’s virtual learning environment.

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/discipline 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. 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) may be granted an appropriate level of access or be permitted to use the school’s facilities at the headteacher’s discretion.

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

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.

8. 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.

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 use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

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 ICT facilities.

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

8.3 Data protection

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

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 Calderdale IT Support Services after consultation with the Headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher immediately.

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

8.5 Encryption

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

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

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Calderdale IT Support Service.

9. Protection from cyber attacks

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

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Calderdale IT Support Services put controls in place that are:
 - **'Proportionate'**
 - **Multi-layered**
 - **Up to date**
 - **Regularly reviewed and tested**
- Automatic, daily back up of critical data takes place and this is stored in the cloud
- Delegated specific responsibility for maintaining the security of our management information system (MIS) to Calderdale IT Support.
- 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
- › 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

10. Internet access

The school wireless internet connection is secured.

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 headteacher.

The headteacher 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)
- › Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

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

11. Monitoring and review

The Headteacher monitors the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: Facebook cheat sheet for staff

Don't 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 not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- › Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- › Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- › The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- › **Google your name** to see what information about you is visible to the public
- › Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- › Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if...

A pupil adds you on social media

- › In the first instance, ignore and delete the request. Block the pupil from viewing your profile

- › Check your privacy settings again, and consider changing your display name or profile picture
- › If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- › Notify the senior leadership team or the headteacher about what's happening

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 2: Acceptable use of the internet: agreement for parents and carers

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

The school uses the following channels:

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

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

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

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

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups 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

Name.....

Signed.....

Appendix 3: Acceptable use agreement for Key Stage 2 Pupils

- I will take care when using the school IT equipment and use it responsibly.
- I will keep my passwords private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images or messages.
- I will not interfere with anyone else’s passwords, settings or files on the computer.
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I know I need permission to take someone’s photograph or to video them.
- Any messages I post online or send in an email will be polite and responsible.
- I will not send or forward messages or create material which is deliberately intended to upset other people.
- I know I must take care about giving away my personal information and making contact with people I do not know when using the internet.
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may happen even if the activity was done outside school.

Pupil name.....

Signed.....

Relationship to child.....

Appendix 4: Acceptable use agreement for Key Stage 1 Pupils

- I will look after all the school IT equipment and use it properly.
- I will only share my username or password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections.
- Any work I upload to the internet will be my own.
- I will only take a photograph or video of someone if they say it is alright.
- All of the messages I send will be polite.
- I will not post anything online which upsets other people.
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet.
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name.....

Signed.....

Relationship to child.....

Appendix 5: Acceptable use agreement for EYFS Pupils

- I will take care when using the school IT equipment and use it properly.
- I will only share my username or password with trusted adults.
- I will tell an adult if I see anything which upsets me.
- I will use a safe name and not my real name on the internet.
- I will only take a photograph or video of someone if they say it is alright.
- Any messages I send will be polite.
- I will not deliberately write anything which upsets other people.
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment.
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school.

Pupil name.....

Signed.....

Relationship to child.....

Appendix 6: Acceptable use agreement for staff

I confirm that I have read and understood the Acceptable Use Policy for staff at Hebden Royd CE Primary School and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document. In particular:

Any content I post online (including outside school time) or send in a message will be professional and responsible and maintain the reputation of the school.

To protect my own privacy, I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents.

If I use any form of electronic communication for contacting pupils or parents I will use the school's system, never a personal account.

I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager.

I will never use my personal mobile phone or other personal electronic equipment to photograph or video pupils.

Taking photographs and videos will only be done with the permission of pupils and/or their parents for agreed school activities.

I will take all reasonable steps to ensure the safety and security of school IT equipment which I take off site and will remove anything of a personal nature before it is returned to school.

I will take all reasonable steps to ensure that all personal laptops and memory devices are fully virus protected and that protection is kept up to date.

I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

I confirm I have read the Acceptable Use Policy and Information Security Guidance for Staff and will implement the guidelines indicated. In particular:

Confidential school information, pupil information or data which I use will be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended.

I understand that I have the same obligation to protect school data when working on a computer outside school.

I will report immediately any accidental loss of personal or sensitive information so that appropriate action can be taken.

I understand that the school may monitor or check my use of IT equipment and electronic communications.

I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name.....

Signed.....

Date.....

Appendix 7: Acceptable use agreement for governors, volunteers and visitors

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- > Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- > Use them in any way which could harm the school's reputation
- > Access social networking sites or chat rooms
- > Use any improper language when communicating online, including in emails or other messaging services
- > Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- > Share my password with others or log in to the school's network using someone else's details
- > Share confidential information about the school, its pupils or staff, or other members of the community
- > Access, modify or share data I'm not authorised to access, modify or share
- > Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT 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.

Name.....

Signed.....

Date.....

Appendix 7: Glossary of cyber security terminology

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
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.