Fairhaven CE VA Primary School

Internet Acceptable Use Policy

Date Approved by Governors:	06/07/2023
Date Agreed by staff:	05/06/2023
Date for Review:	Summer 2025

Signed *Ian Campbell* **Date** *6th July 2023*

Chair of Governors

Contents

Appendices

Vision Statement

Our Christian school community strives to provide a variety of learning experiences for all our young people. We are here to nurture the gifts God gives us and to celebrate our differences. We encourage our pupils to explore their interests, find their talents, flourish and live life to the full. We want our children to live great lives and ultimately make a difference in the world.

Belief – Friendship – Diversity - Achieve
At Fairhaven we want everyone to be the very best they can be.

Statement of Intent

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, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could 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 policies on data protection, online safety and safeguarding
- Prevent disruption that could occur 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.

2. Relevant 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 2022
- 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
- UKCIS 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 which may become available in the future which is provided as part of the school's ICT service

Users: anyone authorised by the school to use the school's 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 agreed by an authorised user

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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.
See Appendix 4 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the 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 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
- 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 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 school's ICT facilities
- Removing, deleting or disposing of the 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 school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The headteacher will use their 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 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 pupil behaviour or staff code of conduct. A copy of our pupil behaviour policy is available on the school website. Staff are given a printed copy of the staff code of conduct at the beginning of every academic year and copies of this are also available in the staff room.

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

5.1 Access to school ICT facilities and materials

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

Computers, Chrome books and laptops
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 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 inform the school office, who will in turn request support from Net Central.

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 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 office staff immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) 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.

At the current time, the school does not have the facility to record telephone calls.

Staff who would like to record a phone conversation should speak to the headteacher and permission may then be given. In this instance the recording must be pre-approved and consent obtained from all parties involved.
Examples of where permission may be granted is given below:

- 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
- Discussing requests for term-time holidays

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. The headteacher 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/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 are also permitted to use their personal devices such as mobile phones in line with the school’s Staff Code of Conduct.

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 use of social media 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.

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).

Our remote access is managed by Net Central. Requests for remote access must be made to the headteacher.

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 the headteacher and ICT manager may require 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. Our data protection policy is available from the school office.

5.4 School social media accounts

The school has an official Facebook and Twitter account, managed by 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 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

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school uses Surf Protect to filter and monitor online use. Parents/carers are made aware of this via the Acceptable

Pupil Technology Acceptable Use Agreement for Pupils/Carers. (Appendix 2).

The effectiveness of any filtering and monitoring will be regularly reviewed.
Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and ICT manager, as appropriate.

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

The governing board will regularly review the effectiveness of the school's monitoring and filtering systems.

6. Pupils

6.1 Access to ICT facilities

Computers and laptops are available to pupils only under the supervision of staff.

Pupils will be provided with an account linked to Google Classroom. They can access this from any devise, at home or at school. Remote learning is delivered via Google Classroom.

6.2 Mobile Phones

Pupils are not permitted to bring mobile phones to school. Pupils are not allowed to bring mobile phones to school. If pupils are known to have a mobile phone in school this will be confiscated and held in the school office until the end of the day. Parents/carers will be informed of the school's policy.

6.3 Smart Watches with cameras

Pupils are not permitted to bring smart watches with camera facilities to school. If pupils are known to have a smart watch in school this will be confiscated and held in the school office until the end of the day. Parents/carers will be informed of the school's policy.

6.4 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) 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 social media channels.

7.3 Communicating with parents 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 in the same way that information about homework tasks is shared.

In particular, staff will let parents know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents 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 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. Passwords include at least one capital letter, one lower case letter, one number and one special character. Staff should use different passwords for each online account.

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.

Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

New members of staff will be given training on creating and storing passwords correctly, If a member of staff leaves the school their online accounts will be de-activated.

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 school's data protection policy. A copy of the school's data protection policy is available form the school office.

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 our IT provider

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 office staff 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 headteacher. Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by Net Central.

9. Protection from cyber attacks

Please see the glossary (Appendix 4) to help you understand cyber security terminology.

The school will:

- Work with governors and the Net Central 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 (such as 360 degree safe) [insert frequency – at least annually], to objectively test 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 – this is automatically stored and backed up daily using Red Store. The school has two hard dries which are changed fortnightly.

- Our management information system (MIS) is provided by Pupil Asset. We delegate the responsibility of maintaining the security of this information to Pupil Asset.
- 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 checking if they have the Cyber Essentials certification
- The School's Disaster Recovery Plan details how we respond to internet related incidents. This is reviewed annually. Net Cenral will be informed immediately. They will be responsible for contacting Action Fraud. If internal channels of communication go down, Pupil Asset will be able to contact parents/carers.
-

10. Internet access

The school's wireless internet connection is secure and filtering arrangements in place. We are aware that filters and not fool proof and staff should report inappropriate sites immediately to the office team. They in turn will contact Net Central who will amend the filtering system.

10.1 Pupils

Pupils are not given the WiFi code.

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 Friends of Fairhaven Committee.

- 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 and ICT manager (Net Central) 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 two years.

The governing board is responsible for approving this policy.

12. Related policies

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

- Online safety Policy
- Cyber-Security Policy
- Data Protection Policy
- Confidentiality Policy
- Photograph and Images Policy
- Remote Education Policy
- Device User Agreement

Other related policies

- Whistleblowing Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures

Staff Device User Agreement

“Belief – Friendship – Diversity - Achieve”

Devices user agreement – staff

Fairhaven Primary has created this agreement to ensure that staff understand their responsibilities when using school-owned devices, such as laptops and chrome books, whether on or off the school premises.

Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined.

The school

Fairhaven Primary School retains sole right of possession of any school-owned device and may transfer the device to another teacher if you do not fulfil the requirements of this agreement.

Under this agreement, the school will:

- Provide devices for your sole use while you are a permanent full-time or part-time teacher at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network.
- Ensure the relevant persons (Net Central) have installed the necessary security measures on any school-owned device before your use – including, but not limited to, the following:
  - Firewalls
  - Malware protection
  - User privileges
  - Filtering systems
  - Password protection and encryption
  - Mail security technology
  - Tracking technology
- Ensure that all devices undergo the following regular checks and updates by the Net Central, including:
  - Termly updates to malware protection
  - Termly software updates
  - Annual password re-set requirements
  - Termly checks to detect any unchanged default passwords
  - Malware scans in line with specific requirements
- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.

- When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage is a result of your own negligence.

Under this agreement, you will:

- Bring the device and charging unit to the school each day and keep the device with you, or within your sight, at all times.
- Transport the device safely using the cover and carry case, if necessary, issued with the device.
- Not permit any other individual to use the device without your supervision, unless agreed by the headteacher.
- Take responsibility for any other individual using the device.
- Always provide suitable care for the device and not do anything that would permanently alter it in any way.
- Lock the device screen when not in use with a passcode.
- Keep the device clean.
- Store devices in a lockable cupboard when not in use.
- Immediately report any damage or loss of the device to the headteacher.
- Ensure any tracking technology applied is active at all times.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the office staff or headteacher.
- Be prepared to cover the insurance excess, repair, or replacement of the device when the damage or loss has been a result of your own negligence.
- Return the device and passcode to the headteacher if your employment ends.
- In the event of long-term illness discuss with the headteacher whether you will require your school device during this time.
- Only use the devices that have been permitted for your use by the headteacher.
- Only use devices for educational purposes.
- Only use apps that are GDPR-compliant and from reputable sources.
- Ensure that any personal data is stored in line with the GDPR.
- Only store sensitive personal data on your device where absolutely necessary and which is encrypted.
- Ensure any school data stored on a device is encrypted and pseudonymised.
- Give permission for the headteacher to erase and wipe data off your device if it is lost, or as part of exit procedures.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties unless permission has been sought from the headteacher.
- Not install any software onto your device unless instructed to do so by the headteacher.
- Ensure any school device you use is running up to date anti-virus software installed. Only use Google Classroom or the class email address to communicate with pupils or parents.

- Not use your school device to send any inappropriate messages, images, or recordings.
- Ensure that your device does not contain inappropriate or illegal content.
- Only access social media sites as approved by the headteacher on your device, and ensure they are used in accordance with the Technology Acceptable Use Agreement.
- Allow the headteacher to monitor your usage of your device, such as internet access, and understand the consequences if you breach the terms of this agreement.

Insurance cover provides protection from the standard risks whilst the device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave the device unattended, and it is stolen, you may be liable for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the device being returned to the school and serious breaches may result in disciplinary action.

Use of personal devices such as mobile phones and tablets are detailed in the School Staff Code of Conduct.

Staff agreement

By signing the below, I certify that I have read and understood this agreement and ensure that I will abide by each principle, including those set out in the Technology Acceptable Use Agreement for Staff.

Signed		**Date**	
Print name		**Device model and number**	

Headteacher approval

Signed		**Date**	
Print name			

Acceptable Use Agreement for Pupils

“Belief – Friendship – Diversity - Achieve”

Technology Acceptable Use agreement

At Fairhaven Primary we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.

I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

I will not:

- ✘ Tell another pupil my username and password.
- ✘ Share personal information, such as my age and where I live, about myself or my friends online.

- ✘ Access social media, such as Facebook and WhatsApp.
- ✘ Speak to strangers on the internet.
- ✘ Take photos of myself or my friends using a school device.

Please read each statement and provide a tick to show that you agree, and then write your name below.

✓

□ I understand why it is important to use technology safely and correctly.

□ I understand my responsibilities when using technology.

□ I understand that I may not be allowed to use technology if I do not use it safely and correctly.

□ I will follow these rules at all times.

Pupil name (please print): ______________________________

Date: ______________________________

Parent name (please print): ______________________________

Parent signature: ______________________________

Date: ______________________________

Pupil Device User Agreement

“Belief – Friendship – Diversity - Achieve”

Device user agreement for pupils

This agreement is between Fairhaven Primary School and ______________________ and is valid for the academic year of 2023/2024. The device is the property of the school and can be monitored.

We have created this agreement to make sure you understand how devices must be used. If you do not follow this agreement, you will be disciplined and may have your device taken off you.

General use principles

- The device belongs to the school and is given on loan to you.
- The device should be brought to school fully charged every day.
- The device should be carried with you during all classes and stored safely in your locker during lunch, break times or sport.
- The device should be taken home with you at the end of the day – it should not be left in your locker overnight.
- You should never leave the device unattended. Unattended devices will be collected and stored in the school office.
- If you leave the school before completing the school year, you must return the device to your teacher.
- If the device is damaged, lost or stolen you must report it to a staff member immediately.
- If you think the device has been stolen, you must report it to the police and tell a staff member.
- If you lose or damage any covers, chargers or other equipment for the device, you must replace it.
- If you damage or lose the device, you must pay for a replacement or repair costs.
- You must not use your device around food or drink.

The school will:

- Make sure the device is secure and has password-protection.
- Monitor your usage of the device to make sure it is being used correctly.
- Make sure all data is backed up securely and remove data every year.

You will:

- Use all devices appropriately and responsibly.
- Only use your device for educational purposes.
- Not play any games on the device during the school day.
- Make sure sounds are muted and not play any music, unless the teacher gives you permission to do so.
- Store devices safely.
- Obey school rules for behaviour and communication on devices.
- Follow this agreement and take care of devices.
- Follow any instructions from staff.
- Give the device back to your teacher at the end of the school year.
- Use any electronic communication appropriately.
- Only access the school’s Wi-Fi with permission from your teacher.

You will not:

- Modify the device in any way, unless a staff member has given you permission to do so.
- Apply marks, stickers or other decorations to the device.
- Give devices to other pupils.
- Remove any covers from the device.
- Sync the device with any computer.
- Delete browsing history from the device.
- Disable any applications on the device, such as tracking.
- Access any websites that you have not been given permission to do so.
- Send any inappropriate messages.
- Send, access or upload any inappropriate images and videos.
- Access any other pupil’s account or files on the device.

Please read each statement and provide a tick to show you agree to the terms, then provide your name below.

☐ I will use my device appropriately.
☐ I will follow this agreement at all times.
☐ I understand that if I do not follow this agreement my device may be taken off me and there may be other disciplinary actions.

Pupil name (please print): ____________________

Date: ____________________

Parent name (please print): ____________________

Parent signature: ____________________

Date: ____________________

National Cyber Security Centre

NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the **@NCSC** Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit **www.ncsc.gov.uk/glossary**.

Antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet

A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)

An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud

Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security

The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)

When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint

A 'footprint' of digital information that a user's online activity leaves behind.

Encryption

A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device

Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Firewall

Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)

Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro

A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching

Applying updates to firmware or software to improve security and/or enhance functionality.

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 makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering

Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan

A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting

Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

Zero-day

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

For more information go to www.ncsc.gov.uk @ncsc