Farley Hill Primary School

ICT and internet acceptable use policy

Responsibility: Full Governing Body	Approved: March 2026
	Review Date: March 2027

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 3
3. Definitions 3
4. Unacceptable use 5
5. Staff (including governors, volunteers, and contractors) 6
6. Pupils 10
7. Parents/carers 12
8. Data security 13
9. Protection from cyber attacks 14
10. Internet access 15
11. Monitoring and review 16
12. Related policies 16
Appendix 1: Acceptable use of the internet: agreement for parents and carers 17
Appendix 2: Acceptable use agreement for older pupils 18
Appendix 3: Acceptable use agreement for younger pupils 19
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors 20
Appendix 5: Glossary of cyber security terminology 21

---

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 the senior leadership team), 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/carers and governors
- Establish clear expectations for the way all members of the school community engage 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our Behaviour Policy, Staff Disciplinary Policy, Staff Code of Conduct and our AI policy.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, 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
- Data (Use and Access) Act 2025
- 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 2025
- 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
- Meeting digital and technology standards in schools and colleges
- Preventing and Tackling Bullying and Cyberbullying Advice for Headteachers and Staff
- Safeguarding learner from radicalisation

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 (including AI), 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 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 5 for a glossary of cyber security terminology.

4. Roles and Responsibilities

4.1 Governors

- the approval of the ICT and Internet Acceptable Use policy
- Ensuring it is implemented and effectiveness is reviewed
- Consider whether to appoint an Online Safety governor

Governors will:

- All governors will ensure they have read and understood the policy
- Meet with the Computing Lead (ICT Strategy meetings)
- Monitor the schools use of their filtering and monitoring protocols
- Keep up to date with school online safety matters
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations.

4.2 Headteacher

- Ensure the safety, including online safety and the use of filtering monitoring protocols, of members of the school community (the day-to-day responsibility may be delegated to the Online Safety lead, Computing lead or another appropriate member of staff).
- Ensure staff with online responsibilities receive suitable and regular training enabling them to fulfil their roles and to train other colleagues
- The Senior Leadership Team (SLT) received regular monitoring reports
- There is a clear procedure to be followed in the event of a serious online allegation being made against a member of staff

4.3 Online Safety Co-Ordinator (Computing lead)

- Day to day responsibility for online issues
- Takes a leading role in in establishing and reviewing the school online and acceptable use policy
- Provide training and advice for staff and ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provide materials and advice for integrating online safety within schemes of work and check that online is taught on a regular basis
- With other colleagues liaise with the Local Authority and the school's technical support team
- Ensure that online incidents are reported, logged and used to inform future online developments
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with school policy
- Report to the Governors (ICT Strategy meetings)
- Report regularly to the SLT

4.4 Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk . SLT should be informed where school policies may require updating.

4.5 External ICT provider

- Ensure, with school staff, that all reasonable measures have been taken to protect the school's network
- Ensure the appropriate and secure use of school equipment

- Protect school data and personal information

This will include

- Working with the school to ensure the appropriate level of security protection procedures such as filtering and monitoring, which are reviewed and updated on a regular basis. Any misuse or attempted misuse is reported to the Headteacher and Computing Lead for investigation or action.
- The ICT infrastructure is secure and protected from misuse or malicious attack and updated regularly
- Conduct a full security check and monitor the school's ICT systems on a regular basis
- The school meets the online technical requirements outlined in any relevant local authority online policy/guidance
- Users may only access the school's network(s) through a properly enforced password protection policy, in which passwords are regularly changed
- Online technical information is kept up to date, applied as necessary and passed onto others where relevant
- Appropriate steps are taken to protect personal information and secure data on all devices and removable media
- Provide secure access to the school network from home where necessary using VPN or other technologies
- Block access to potentially dangerous sites and, where possible, prevent the download of potentially dangerous files

5. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities and applies to all staff, Governors, pupils, ICT support teams, volunteers and contractors.

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 any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- 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
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- 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 internet and 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
- Using AI without due diligence and sharing information inappropriately through AI (see school AI policy)

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher and Governors 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.

5.1 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.

- Written approval would need to be granted by the Headteacher prior to the use of school ICT facilities via email. This would include approval for use of software or AI programmes not explicitly agreed in the school's AI policy.

- A written request would need to be given to the Headteacher, Deputy Headteacher or appropriate Governor before the school's ICT facilities are used. Written approval would be given or not as appropriate.

5.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour, staff disciplinary and staff code of conduct. This could include revoking any permissions the user may have to use the school's systems.

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

6.1 Access to school ICT facilities and materials

The School's Business Manager (SBM) and ICT technical support team 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
- AI policy clearly states which AI programmes should be used for school related tasks and how they should be used

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 contact the School Business Manager.

6.1.1 Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Maintain an understanding of current online safety matters
- Implement this policy consistently – annually signing the Staff Acceptable Use Policy (AUP) to indicate agreement
- Ensure pupils understand and follow the schools ICT and Internet Acceptable Use policy
- Report and log any suspected misuse or problem to the appropriate colleagues for investigation and action.
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy. Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline (maintaining an attitude of it could happen here).
- Digital communications with pupils MUST be on a professional level and only carried out on school approved systems
- Recognise that online issues are embedded in all aspects of the curriculum and other school activities and that pupils have a good understanding of research skills the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- Monitor ICT activity in lessons, extra-curricular and extended school activities. Pupils should be guided to sites checked as suitable for use and staff are aware of how to deal with any unsuitable material that is found in internet searches
- Use equipment and devices for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations e.g. visible on car seats.
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. Passwords must:
  - Not be shared with others and must be changed regularly
  - Be suitably strong, in accordance with the school's password policy
  - Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by the School Business Manager or ICT Technical support team
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- Report any loss, theft, damage or compromise of a school device promptly to the School Business Manager, Headteacher and designated safeguarding lead and data protection officer

This list is not intended to be exhaustive.

6.1.2 Use of phones and email

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

This email account should be used for work purposes only. Staff must make sure multi-factor authentication is enabled 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 subject access requests from individuals under the UK GDPR and 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 using a strong, state-of-the-art encryption standard 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 School Business Manager and Data Protection Officer immediately and follow our data breach procedure.
- Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

6.2 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, members of the SLT or School Business Manager 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 and 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 or tablets) in line with the school's same criteria set out for use of school's ICT facilities (see above). Phones must not be present in front of pupils.

Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

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 and use of email (see section 6.2.1) to protect themselves online and avoid compromising their professional integrity.

6.2.1 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 and set to Private.

The school has guidelines for staff on appropriate security settings for social media accounts.

6.3 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).

The school uses a VPN known as Remote Desktop Access. This is managed by our ICT Technical Support team and must be on all devices staff use remotely. Staff can request remote access through the Headteacher and School Business Manager. Remote access should only be used for drives you have access to and that are required for your job role. Users should not attempt to browse or explore network areas unrelated to your work.

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 as the ICT technical team, SBM and Headteacher 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.

Data Protection Policy

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

To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and 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 school personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes:

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing

- To comply with any legal obligation

The list above is not exhaustive.

The school monitors ICT use in order to:

- Obtain information to ensure pupils remain safe online in school
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) and Computing Lead will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and School Business Manager as appropriate.

6.5 Reporting of Misuse

Where a staff member misuses the school's ICT systems or the internet, or misuses of a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

For staff, Governors, volunteers and contractors the school will consider if misuses of the school's ICT systems or the internet, or misuses of a personal device involves illegal activity or content, or otherwise serious incidents, should be reported to the police.

6.6 Reporting of Misuse

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- Children can abuse their peers online through: abusive, harassing, and misogynistic messages, non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups, sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

7. Pupils

7.1 Access to ICT facilities

- Computers and equipment are available to pupils only under the supervision of staff
- Email addresses and passwords are provided to pupils, for educational purposes only. Pupils must not share their passwords with others, or use their email account to share or download files, including software from the Internet or inappropriate content, without the permission of the school staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL https://farleyhill-wokingham.frogos.net

7.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with our Behaviour policy and the NetSmart Code of Practice (for EYFS, KS1 and KS2) 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

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident and will be proportionate.

8. Parents/carers

8.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers 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/carers are granted access in this way, they must abide by this policy.

Parents must:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following orgnisations and websites:

  What are the issues – UK Safer Internet Centre

  https://saferinternet.org.uk/guide-and-resource/what-are-the-issues

  Hot Topics – Childnet International

  https://www.childnet.com/blog/hot-topics-finding-more-information-about-the-topics-affecting-young-people/

  Parents Resource Sheets – Childnet International

  https://www.childnet.com/resources/parents-and-carers-resource-sheet/

  Healthy Relationships – Disrespect Nobody

  https://www.gov.uk/government/collections/disrespect-nobody-campaign

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Learning Platform. This policy will also be shared with parents. Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

8.2 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/carers 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/carers to sign the agreement in appendix 1.

8.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

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

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

9. 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 cybercrime technologies.

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

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

9.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users must not use the same passwords across multiple platforms.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.

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.

9.2 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 should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the Headteacher, School Business Manager and the ICT technical support team.

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 incoming files should always be virus-checked by the ICT technical team before they are downloaded.

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

9.3 Data protection

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

Data Protection Policy

9.4 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 School Business Manager and the ICT technical Support team

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 School Business Manager or 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 shut down completely at the end of each working day.

9.5 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. This should not be needed as there is the VPN access.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by theSchool Business Manager and the ICT Technical Support team

10. Protection from cyber attacks

Please see the glossary (appendix 5) 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 all users, including staff, pupils and governors (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:
  - The methods hackers use for tricking people into disclosing personal information, including phishing
  - Online safety and password security
  - Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
  - The physical security of devices, for example not leaving a laptop unlocked and unattended
  - The risks of using removable storage media, such as USBs
  - Multi-factor authentication
  - How and when to report a cyber incident or attack
  - How and when to report a data breach
  - Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
  - How to check the sender address in an email
  - How to respond to a request for bank details, personal information or login details

- How to 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) 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 (process typically daily via ICT Technical support with Softegg) and store these backups on [cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the ICT Technical Support Team
- 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
- Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)
- Make sure effective cyber breach prevention measures and processes are in place, e.g. endpoint detection and response systems
- 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 (or a similarly effective and recognised) 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 and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with Wokingham Borough Council to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred

11. Internet access

The school's wireless internet connection is secure.

- The school has a securely filtered and monitored wi-fi for staff and pupil use and a guest wi-fi which has some filtering and monitoring assigned
- There is a filtering and monitoring protocol in place for the use of all school ICT equipment including iPads, Windows devices and Chromebooks

- If any inappropriate site is not identified by the filter the staff and children are aware of the school procedures to report this site/s

11.1 Parents/carers and visitors

Parents/carers 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/carers 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 Guest 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 School or Guest WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

12. Monitoring and review

The Headteacher, Governors, Computing Lead, SLT and School Business Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The governing board is responsible for reviewing/approving this policy.

12.1 Complaints against internet use

Any complaints relating to internet misuse should be made in accordance with the school's existing complaints policy.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

12.2 Sanctions

Failure to comply with the requirements of this policy will be dealt with as by the school's existing policies on behaviour and staff disciplinary.

The use of the compute systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

12.3 Related policies

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

- Social media
- Safeguarding and child protection
- Behaviour
- Staff Disciplinary
- Data protection
- Remote education
- Artificial Intelligence (AI)

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Email • Arbor Parent Portal • 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 or wider social media to complain about or criticise members of staff or the school. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way directly with the school. • Use private groups, the PTA Facebook page, or personal social media including WhatsApp to complain about, or try to resolve, a school-related 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 event in school that would include other children, unless I have the permission of the other children's parents/carers. This is to respect the privacy of all the families in the school.	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails or on the Learning Platform • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the school's network using someone else's details • Bully other people I will only use an AI tool (Microsoft CoPilot when in school under staff supervision). I will not use an AI tool during assessments, including internal and external assessments, and homework or to present AI-generated text or imagery as my own work. If I use AI will not use any personal data or information about myself, my peers at school, staff or the school itself, including the school's name. I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately shut the device screen or turn the device over (iPad) and let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can use sanctions if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can sanction me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

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

- Access, or attempt to access any illegal or 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 any private business, 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.

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

Appendix 5: 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. Many of these terms are from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure 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	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised 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 who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
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 with the end aim of fixing them.

TERM	DEFINITION
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 or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
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.