IT and internet acceptable use policy

Including: Online Safety Filtering and Monitoring and AUPs
Addendum to the Child Protection and Safeguarding Policy

Bowdon Church School

Model Policy taken from The Key

Approved by forbessolicitors.

Prepared by SMoss (Deputy Headteacher) in consultation with V Hardman (School Business Manager)

Reviewed at least annually, or more regularly in response to any significant new technological developments or trends in technology-related behaviours, particularly concerning Artificial Intelligence

Approved by:	Governing Board	**Date:**
Last reviewed on:	June 24, September 2025	
Next review due by:	September 2026	

Contents

1. Introduction and aims

Information technology (IT) 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 IT 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 IT resources for staff, pupils, parents/ carers 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 IT systems
- Support the school in teaching pupils safe and effective internet and IT use

This policy covers all users of our school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy will be dealt with under our behaviour policy, staff code of conduct or parent code of conduct.

2. Relevant legislation and guidance

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

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

3. Definitions

- **IT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's IT service
- **Users:** anyone authorised by the school to use the school's IT 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 IT facilities

- **Materials:** files and data created using the school's IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the school's IT facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright
- Using the school's IT 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 IT 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 IT 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 IT facilities
- Causing intentional damage to the school's IT facilities
- Removing, deleting or disposing of the school's IT 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 tools and generative chatbots (such as ChatGPT and Google Bard): To write homework or class assignments, where AI-generated text or imagery is presented as pupil's own work
- Using AI tools not approved in the AI policy
- To enter any personal information (personal data, intellectual property or private information (including commercially sensitive information, such as contracts) into any Generative AI model that might breech the Data Protection Policy as any information entered into a Generative AI model is no longer private or secure.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The head teacher or deputy head teacher 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 IT facilities.

4.1 Exceptions from unacceptable use

Where the use of school IT 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.

Acceptable use of artificial intelligence (AI) tools, for example:

Pupils may use AI tools and generative chatbots:

- If listed in the appendix of the AI Policy
- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed
- Staff who wish to utilise AI tools must ensure that the potential new use is assessed to consider if a Data Protection Impact Assessment is required and follow the school Data Protection Policy. The AI tools must be approved by the AI lead or listed in the AI policy appendix
- Staff are permitted to explore and utilise AI-based tools and technologies to assist in managing their work providing they adhere to the AI Policy. Examples of such tasks may include marking and feedback, report writing, lesson planning, professional development and facilities management. AI can provide valuable support while still incorporating professional judgement and expertise. AI tools will be used responsibly, ensuring they complement staff professional judgement and expertise, without replacing them.

4.2 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 code of conduct policy.

Specific sanctions in place for unacceptable IT use:

- Permission revoked to access the school network or internet.
- Permission to use a mobile device, such as a chrome book or iPad revoked and limited to access in the IT suite only.

School behaviour policy and mobile phone can be found on the school website here: https://www.bowdoncs.org.uk/policies/

Staff code of conduct and staff discipline policy can be found on the school network

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

5.1 Access to school IT facilities and materials

The school's school business manager (SBM) , Mrs V. Hardman, manages access to the school's IT facilities and materials for school staff with support from HG- IT Support Service. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's IT 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 by email.

For access to the Google Drive, to reset passwords for Gmail staff should email or speak direct to Mrs. Moss (Deputy Head teacher) or to HG- IT Support Service.

5.1.1 Use of phones and email

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

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

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

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

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

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

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

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

If staff send an email in error that contains the personal information of another person, they must immediately inform the School Business Manager and Global Policing directly either by e-mail or telephone and follow our data breach procedure.

Data Protection Officer: Shane Williams

Email: datarequests@globalpolicing.co.uk

Web: www.globalpolicing.co.uk/data

Telephone: 0161 510 2999 (Option 2)

Staff must not give their personal phone number(s) to parents/carers or pupils. In an emergency, when off site, if a personal phone is used, staff should dial 141 before the number in order to withhold their personal number. Staff must use phones provided by the school to conduct all work-related business when in school. However staff may need their phone for 2 step ID verification to access CPOMs so should do so in an office, or out of the sight of children.

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 IT acceptable use as set out in section 4.

Staff are expected at all times to adhere to the BCS Mobile Phone Policy (on school website)

5.2 Personal use

Staff are permitted to occasionally use school IT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The head teacher 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 teaching hours
- 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 IT 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 IT facilities for personal use may put personal communications within the scope of the school's IT 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 BCS Mobile Phone Policy (on school website).

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

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

5.2.1 Personal social media accounts

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

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

5.3 Remote access

We occasionally allow staff to access the school's IT facilities and materials remotely if required to fulfil their role or due to reasonable adjustments. They should dial in using a virtual private network (VPN).

Managed by: the School Business Manager, supported by HG-IT

- Security arrangements: Access should only be made using a school device to ensure anti-virus protection is up to date and use two factor authentication.

- Protocols for remote access are the same as in school. Access only allowed for designated staff to fulfil their role.

- Only the head teacher can give permission to set up remote access.

Staff accessing the school's IT 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 IT facilities outside the school and must take such precautions as the SBM/ head teacher may require against importing viruses or compromising system security.

Our IT 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.

School's data protection policy https://www.bowdoncs.org.uk/data-protection-1/

5.4 School social media accounts

The school has an official Twitter account, managed by Mrs S Thompson (Assistant Head teacher) Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

Photos of individual children are not to be posted unless direct permission has been given by parents and any other group images must have parental consent, updated annually. Nothing must be posted that would adversely affect the reputation of the school or an individual

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 IT 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 IT 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 IT personnel, head teacher, deputy head teacher, school business manager & safeguarding lead may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

Monitoring system

The school monitors IT use in order to:

- provide a safe environment in line with safeguarding requirements (KCSIE) to learn and work, including when online

- Investigate compliance with school policies, procedures and standards
- Ensure effective school and IT 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 and follow recommendations from HG- IT support (Jonathon Gandy: jonathon.gandy@hg-it.co.uk or support@hg-it.co.uk) Both systems are cloud based and the switches located in the server room.

o Monitoring - **SENSO** is the system used for keystroke monitoring - The system tracks keystrokes and reports on any potential concerns via an online dashboard and also via email on high level alerts such as pornographic content. This system is accessed by the School Business Manager, Head teacher as DSL, Pastoral Lead as DSL, and Deputy Head teacher. Each device for Senso has to have a driver installed and only applies to School owned devices.

o Internet Filter - Real-time, content-aware web filtering software and firewall (Smoothwall) will be used in order to minimise the risk of exposure to inappropriate material. **Smoothwall Filtering** applies filtering rules based on a set of user criteria: Pupils, Staff, Visitors, and Nursery. Filtering applies to anything on the network at any given time This reports triggers to School Business Manager (V Hardman), Head teacher (Sam Halliwell) as DSL and Pastoral Lead (Zoe Power) as DSL

- Staff are aware of those systems and trained in their related roles and responsibilities

o For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns

- It regularly reviews the effectiveness of the school's monitoring and filtering systems

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

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and IT manager, as appropriate.

6. Pupils

6.1 Access to IT facilities

- Computers in the school's IT suite, school laptops, Chromebooks and iPads are available to pupils only under the supervision of staff, for educational purposes only.

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out, **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Searching and screening pupils is conducted in line with the DfE's latest guidance on searching, screening and confiscation. https://www.gov.uk/government/publications/searching-screening-and-confiscation

Under common law, school staff have the power to search a pupil for any item if the pupil agrees. The member of staff should ensure the pupil understands the reason for the search and how it will be conducted so that their agreement is informed.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above. Only the head teacher, or a member of staff authorised by the head teacher, can carry out a search. The head teacher can authorise individual members of staff to search for specific items, or all items set out in the school's behaviour policy.

Authorised members of staff will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the head teacher / deputy head teacher / designated safeguarding lead
- Consider the age and needs of pupils being searched or screened. This includes the individual needs or learning difficulties of pupils with Special Educational Needs (SEN) and making reasonable adjustments that may be required where a pupil has a disability.
- Consider using CCTV footage to decide whether to conduct a search for an item.

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the school behaviour policy (School website: https://www.bowdoncs.org.uk/policies/)

- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / head teacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

Not view the image

Not copy, print, share, store or save the image

- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy
- Searching, screening and confiscation: guidance for schools

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of IT 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 IT or the internet to breach intellectual property rights or copyright
- Using IT 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 IT facilities
- Causing intentional damage to the school's IT 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

For Sanctions – see section 4.2 above

7. Parents/carers

7.1 Access to IT facilities and materials

Parents/carers do not have access to the school's IT 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 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/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 electronically sign the Acceptable Use Policy on behalf of their child via a Google Form.

7.3 Communicating with parents/carers about pupil activity

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

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

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

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

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's IT 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 IT facilities should set strong passwords for their accounts and keep these passwords secure.

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

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

Teachers will keep children's passwords for required sites in a secure location in case pupils lose or forget their passwords.

Google Accounts

- The Deputy Head teacher (Sue Moss) and HG- IT support oversee and create accounts as required.
- Accounts are only set up once parental permission has been given via a Google Form.
- Users can set their own passwords but a password reset request is managed by the Deputy Head teacher.

- All children are set up with a school Google account, which is managed by their parents/carers in order to access Google Classroom or for Year 5/6 children to use the school Chromebooks. Children may be required to access this account under staff supervision to complete tasks. Class teachers may need to keep a record of passwords, in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's IT 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 IT 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. The school data policy can be found here: https://www.bowdoncs.org.uk/data-protection-1/

Data Protection Officer: Shane Williams

Email: datarequests@globalpolicing.co.uk

Web: www.globalpolicing.co.uk/data

Telephone: 0161 510 2999 (Option 2)

The requirements of data protection will be met by this school as the basis for collecting, storing, accessing, sharing and deleting personal data. Data will be processed fairly, lawfully and in a transparent manner. It will be used for specified, explicit and legitimate purposes in a way that is adequate, relevant and limited. It will be

accurate and kept up to date and kept no longer than is necessary. Data will be processed in a manner that ensures appropriate security of the data.

8.4 Access to facilities and materials

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

These access rights are managed by the School Business Manager, Mrs V. Hardman with support HG- IT support.

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, Mrs V Hardman or a designated DSL 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 the SBM or HG- IT support.

The use of memory sticks or other digital storage media in school is not permitted by pupils and restricted in school to authorised users, only for specific occasions if deemed essential by the school business manager or by the Head teacher.

9. Protection from cyber attacks

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

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: the school will verify this using an audit (such as 360 degree safe) 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 - automatically, once a day, and store these backups on cloud-based backup systems with HG-IT
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to HG- IT support

- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely using a password manager

- Make sure IT 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
- Have a business continuity plan that details the immediate response in the cause of an incident relating to IT, including communications and data
- Work with HG- IT support to see what it can offer the school regarding cyber security,

10. Internet Access

The school's wireless internet connection is secure.

Smoothwall Filtering applies filtering rules based on a set of user criteria: Pupils, Staff, Visitors, and Nursery. Filtering applies to anything on the network at any given time. See section 5.5 above

Separate policies apply for levels of access for staff/ pupils/ parents or carers

All staff must be aware that filters aren't foolproof. Children must be supervised on the internet at all times and staff must report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the School Business Manager in the first instance. If it is a safeguarding concern, alert the DSL –or Headteacher

10.1 Pupils

The use of WiFi by pupils:

- There are separate Wifi networks for pupils and staff, each with their own set of rules and restrictions
- Pupils and staff networks are restricted by Smoothwall - with separate rules and settings as appropriate

10.2 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 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 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 year.

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
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education
- Mobile phone usage
- AI policy

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 guidelines for school staff on Facebook / Social media

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

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

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

A parent/carer adds you on social media

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

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

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

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

To be sent out via Google Forms and recorded electronically at the start of each school year

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/text groups for parents (for school announcements and information) from Arbor ● Our virtual learning platform - Google Classroom Parents/carers sometimes 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).	
I/we agree: When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I/we 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 that they can be dealt with in line with the school's complaints procedure I/we agree we will not: ● Use social media to criticise or complain about members of staff (this includes use of class Whatsapp groups). This approach is not constructive and does not allow the school to improve or address issues that have not been raised through appropriate channels. ● Use social media (including Whatsapp) to complain about, or try to resolve, a behaviour issue involving other pupils and/or parents. Where I wish to raise an issue about a specific behaviour issue or incident related to school, I will contact the school and speak to an appropriate member of staff. ● Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

To be sent out via Google Forms and recorded electronically at the start of each school year

Acceptable use of the school's IT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's IT 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, Instagram, Snapchat, WhatsApp or other social networking sites
- Use chat rooms
- Reveal my own or other people's personal details, such as addresses, telephone numbers or pictures.
- 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, on Google Classroom or in emails
- Send any photos, videos or live streams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work
- Use the school IT equipment (laptops, Chromebooks or Ipads for anything that is not approved by my teacher.

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 IT systems and internet.

I understand mobile phones and devices such as smart watches that can access the internet or send or receive messages, are NOT permitted in school (including my classroom or in my school bag) , on school trips or residentials

.I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's IT 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 IT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

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

To be sent out via Google Forms and recorded electronically to staff / governors / regular volunteers but also available as paper copy for visitors

Acceptable use of the school's IT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's IT facilities and accessing the internet in school, or outside school on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote 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 IT 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 school business 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 IT 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. They're from the National Cyber Security Centre (NCSC) glossary.

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

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.