Oxford Diocesan Schools Trust
St Mary's Convent
Denchworth Road, Wantage
Oxford, OX12 9AU
odst.governance@oxford.anglican.org
www.odst.org.uk

| | |
|---|---|
| **Statutory:** | Policy provided centrally for adoption by schools with minimal amendment to the core text. Changes are allowed to the text where indicated |

# ICT & Internet Acceptable Use Policy

Grove CE Primary School

| | |
|---|---|
| **Approved by:** | **Education Quality Standards & Safeguarding** |
| **Date:** | **June 2026** |
| **Next review date:** | **31 December 2027** |

| | |
|---|---|
| **Adopted by school:** | **LGB** |
| **Date:** | **September 2026** |

# Contents


1. Introduction and aims ..... 3
2. Relevant legislation and guidance ..... 3
3. Definitions ..... 4
4. Safeguarding ..... 4
5. Unacceptable use ..... 5
   5.1. Exceptions from unacceptable use ..... 6
   5.2. Sanctions ..... 6
6. Staff (including LGB members, volunteers, and contractors) ..... 6
   6.1. Access to school ICT facilities and materials ..... 6
      6.1.1. Personal social media accounts ..... 7
   6.2. Remote access ..... 7
   6.3. School social media accounts ..... 8
   6.4. Monitoring and filtering of the school network and use of ICT facilities ..... 8
7. Pupils ..... 9
   7.1. Use of mobile phones ..... 9
   7.2. Access to ICT facilities ..... 9
   7.3. Search and deletion ..... 9
   7.4. Unacceptable use of ICT and the internet outside of school ..... 10
8. Parents/carers ..... 11
   8.1. Access to ICT facilities and materials ..... 11
   8.2. Communicating with or about the school online ..... 11
   8.3. Communicating with parents/carers about pupil activity ..... 11
9. Data security ..... 11
   9.1. Passwords ..... 12
   9.2. Software updates, firewalls and anti-virus software ..... 12
   9.3. Data protection ..... 12
   9.4. Access to facilities and materials ..... 12
   9.5. Encryption ..... 12
10. Protection from cyber attacks ..... 13
11. Internet access ..... 13
   11.1. Pupils ..... 13
   11.2. Parents/carers and visitors ..... 14
12. Monitoring and review ..... 14
13. Related policies ..... 14

Appendix ..... 15

Glossary of cyber security terminology ..... 15

# 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), LGBs, 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 LGB members
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

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

Breaches of this policy may be dealt with under our behaviour policy, staff discipline policy, staff code of conduct and governance code of conduct.

This policy should be read alongside the Online Safety Policy, which sets out education, reporting and safeguarding responses relating to AI-generated harm.

# 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
- 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
- Working together to safeguard children - GOV.UK
- 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
- Mobile phones in schools - GOV.UK

# 3. Definitions

- ICT facilities: all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service including wearable technology such as smart watches, smart glasses, AI-enabled glasses and other devices capable of recording images, audio or video.
- **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 for a glossary of cyber security terminology.

# 4. Safeguarding

This policy addresses the emerging and evolving risks associated with the use of artificial intelligence (AI), mobile and digital technologies in educational settings, ensuring that robust safeguards are in place to protect children from potential harm. In line with Keeping Children Safe in Education, the school recognises that online harm may occur both within and outside the school environment, may be contextual or cumulative, and may involve the use of personal devices, online platforms or AI-enabled technologies.

AI and Digital Tools: The school recognises the potential safeguarding risks posed by AI-driven educational tools and platforms, including risks relating to data protection and privacy, bias and discrimination, the creation or manipulation of content (including AI-generated or "deepfake" images and videos), exposure to inappropriate material, cyberbullying, harassment, misogyny and harmful sexual behaviour. AI-generated content that causes harm, distress or misrepresentation may constitute a safeguarding concern and will be managed in line with the school's safeguarding and child protection procedures.

The school will implement clear guidelines and controls on the use of AI and digital technologies, ensuring that any tools used are appropriately vetted, risk-assessed and compliant with safeguarding, data protection and information security requirements. AI tools must not be used to generate, manipulate, analyse or store pupil images, recordings or personal data unless explicitly approved by the school and subject to appropriate safeguards. The impact of digital and AI-enabled technologies on pupil safety and wellbeing will be regularly reviewed as part of the school's safeguarding arrangements.

AI-generated content such as deepfakes is recognised as a form of child-on-child abuse where it causes harm. Such incidents will be managed as safeguarding concerns and reported to the DSL immediately.

Staff Training and Awareness: All staff will receive regular safeguarding training and updates that include information on the risks associated with digital technologies and AI, as required by Keeping Children Safe in Education 2026. This will include developing staff awareness of emerging online harms, AI-generated abuse (including deepfakes), professional boundaries, and the appropriate response to concerns. Staff are expected to remain vigilant, exercise professional curiosity, and report any concerns promptly to the Designated Safeguarding Lead (DSL).

In line with Working Together to Safeguard Children 2026, this policy explicitly recognises that safeguarding duties apply to all children including those who are unborn, adopted, in kinship care or looked-after, and acknowledges that children may experience multiple and overlapping harms including online harm, exploitation and abuse outside the home.

The school will work proactively with multi-agency partners and share information proportionately and lawfully to support early identification and intervention.

The policy reflects the strengthened emphasis on anti-racist and anti-discriminatory practice. All users must challenge discrimination, misogyny and harmful conduct online. Leaders are responsible for fostering inclusive online cultures and addressing disproportionality in safeguarding concerns.

Please refer to the schools Safeguarding and Child Protection Policy, available on the schools website.

# 5. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 5.1 below).

Unacceptable use of the school's ICT facilities (including unauthorised use of AI tools) includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Intentionally trying to get around or bypass the protections put in place to restrict access to certain websites, apps, or content

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or any other relevant member of staff 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.

### 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 discipline, staff code of conduct and governance code of conduct.

## 6. Staff (including LGB members, volunteers, and contractors)

### 6.1. Access to school ICT facilities and materials

The school's designated IT lead manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

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

#### 6.1.1. 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.

Staff must not give their personal phone number(s) to parents/carers or pupils.

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 5.

In line with Department for Education guidance that schools should be mobile phone-free environments by default, staff are expected to limit the use of personal mobile phones and smart devices during the school day. Personal devices must not be used in classrooms, learning spaces, or in the presence of pupils, except where expressly authorised by the headteacher or senior leadership team for professional, medical or safeguarding reasons. Staff must not use personal devices to communicate with pupils or to take photographs, videos or audio recordings of pupils under any circumstances. Where mobile phones are required for work purposes, school-issued devices or approved systems must be used. Staff are responsible for modelling appropriate behaviour, maintaining professional boundaries, and ensuring that mobile phone use does not compromise safeguarding, data protection, supervision, or the calm and orderly running of the school.

## 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 data protection lead 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 specified times
- 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 6.5). 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 staff code of conduct.

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

Staff should take care to follow the school's policy on use of social media and use of email (see section 6.1.1) 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.

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

## 6.3. Remote access

We allow staff to access the school's ICT facilities and materials remotely. Staff are not permitted to store personal data on personal devices.

The school's designated IT lead will explain the remote access system you use, including:

- Who manages it
- Security arrangements
- Protocols for remote access
- How staff can request remote access

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 school's designated IT lead 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.

## 6.4. School social media accounts

The school has access to an official Facebook account, managed by senior teachers. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school must hold written parental consent for any sharing of photographs of pupils used on social media and in newsletters published by the school.

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

## 6.5. Monitoring and filtering of the school network and use of ICT facilities

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

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

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

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

Our LGB 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 headteacher and/or 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 data protection lead.

# 7. Pupils

## 7.1. Use of mobile phones

In line with Department for Education guidance on the use of mobile phones, and Keeping Children Safe in Education, the school is a mobile phone-free environment during the school day. Pupils must not use mobile phones, smartwatches or other personal internet-enabled or recording devices on school premises, including during lessons, between lessons, breaktimes and lunchtimes, except where a specific exception has been agreed by the school for medical or safeguarding reasons. Where mobile phones are brought onto site, they must be switched off and stored securely in accordance with school procedures. Pupils must not use mobile phones or personal devices to take photographs, make audio or video recordings, access social media, messaging services or AI-enabled tools that could expose themselves or others to harm. Any misuse of mobile phones, including the creation or sharing of harmful, inappropriate or AI-generated content (such as deepfakes), will be treated as a safeguarding or behaviour concern and managed in line with the school's safeguarding and behaviour policies.

## 7.2. Access to ICT facilities

- Computers and equipment in the school are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

## 7.3. 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)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they 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 ODST DSL
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, you should proceed according to your behaviour policy)

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.

- 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 school leaders in conjunction with the ODST DSL 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 / searches and confiscation policy (make sure that your searches and confiscation policy reflects the updated DfE guidance, which came into force on 1 September 2022)

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

## 7.4. Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy], if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Use of AI in contravention to established school agreements, which includes: entering school or pupil data into AI platforms, using AI to make judgements about pupils, using AI generated content without careful checking, entering pupil intellectual property into AI platforms, allowing pupils under 13 to use AI platforms.

# 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 as it applies to staff.

## 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 relevant acceptable use agreement.

## 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 as part of curriculum plans.

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 cyber crime 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 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.

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

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

## 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.

## 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's designated IT lead.

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's designated IT lead 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.

Staff may access their school account for work purposes on a personal device if they follow the policies imposed by their ICT management system (security protocols, password access etc.)

Staff must not store pupil or school data on personal devices or USB drives, or take hard copies of pupil data offsite.

# 10. Protection from cyber attacks

Please see the glossary in the appendix to help you understand cyber security terminology.

The school will:

- Work with the LGB and school leaders 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

Work with ODST to:

- 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 and store these backups on cloud-based backup systems or 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 BromCom
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- 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 at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

# 11. Internet access

The school's wireless internet connection is secure and includes appropriate filtering systems which are monitored. School leaders report information regarding breaches of the filtering system to the LGB.

## 11.1. Pupils

- Pupils will only use the Wifi provided at school through one of the provided laptops or tablets, and will not know the password. No pupil phones will be allowed a connection to the Wifi.

### 11.2. 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.

### 11.3. Camera-enabled wearable devices

Pupils, visitors, contractors, parents/carers and other adults on site must not use camera-enabled smart glasses, AI-enabled glasses, smart spectacles, body-worn cameras or other wearable recording devices capable of capturing images, audio or video unless expressly authorised by the headteacher for a specific educational, accessibility or safeguarding purpose. Any recording functions must be disabled whilst on school premises. Unauthorised recording of pupils, staff or visitors may result in removal from site and may be managed as a safeguarding, privacy or data protection concern.

## 12. Monitoring and review

ODST Trustees review this policy annually and the LGB monitor the implementation, including ensuring it is updated to reflect the needs and circumstances of the school.

## 13. Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff code of conduct
- Data protection

# Appendix

## Glossary of cyber security terminology

| | |
|---|---|
| **Antivirus** | Software designed to detect, stop and remove malicious software and viruses. |
| **Breach** | When your data, systems or networks are accessed or changed in a non-authorised way. |
| **Cloud** | Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices. |
| **Cyber attack** | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously. |
| **Cyber incident** | Where the security of your system or service has been breached. |
| **Cyber security** | The protection of your devices, services and networks (and the information they contain) from theft or damage. |
| **Download attack** | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent. |
| **Firewall** | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network. |
| **Hacker** | Someone with some computer skills who uses them to break into computers, systems and networks. |
| **Malware** | Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations. |
| **Patching** | Updating firmware or software to improve security and/or enhance functionality. |
| **Pentest** | Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses. |
| **Pharming** | An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address. |
| **Phishing** | Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. |
| **Ransomware** | Malicious software that stops you from using your data or systems until you make a payment. |
| **Social engineering** | Manipulating people into giving information or carrying out specific actions that an attacker can use. |
| **Spear-phishing** | A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts. |
| **Trojan** | A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer. |
| **Two-factor/multi-factor authentication** | Using 2 or more different components to verify a user's identity. |
| **Virus** | Programmes designed to self-replicate and infect legitimate software programs or systems. |
| **Virtual private network (VPN)** | An encrypted network which allows remote users to connect securely. |
| **Whaling** | Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation. |