Leeds Diocesan Learning Trust (LDLT)

Company Number 13687278

Acceptable Use and Online Safety Policy

LDLT
LEEDS DIOCESAN LEARNING TRUST

Approved by Board of Directors: 23rd September 2026
Date of Next Review: September 2029
Responsible Officer: CFO

Contents

Vision Statement 2
Other Related Policies 2
1. Introduction and Aims 2
2. Relevant legislation and guidance 3
3. Definitions 3
3. Online-safety Risks 3
3.1 The four areas of online-safety risk 3
3.2 Roles and responsibilities 4
4. Unacceptable Use 5
4.1 Exceptions from Unacceptable Use 6
4.2 Sanctions 6
5. Staff (including governors, volunteers and contractors) 6
5.1 Access to school ICT facilities and materials 6
5.2 Use of phones and emails 6
5.3 Personal Use 7
5.4 Personal social media accounts 7
5.5 Remote access 8
5.6 School social media accounts 8
5.7 Monitoring and filtering of the school network and use of ICT facilities 8
6. Pupils 9
6.1 Access to ICT facilities 9
6.2 Search and deletion 9
6.3 Unacceptable use of ICT and the internet outside of school 11
7. Parents/carers 11
7.1 Access to ICT facilities and materials 11
7.2 Communicating with or about the school online 12
7.3 Communicating with parents/carers about pupil activity 12
8. Data security 12
8.1 Passwords 13
8.2 Software updates, firewalls and anti-virus software 13
8.3 Data protection 13
8.4 Access to facilities and materials 13
8.5 Encryption 13
9. Protection from cyber attacks 14
10. Internet access 15
10.1 Pupils 15
10.2 Parents/carers and visitors 15
10.3 Mobile phones and personal devices 15
Appendix 1: Social Media Guidance for staff 16
Appendix 2: Acceptable use of the internet: agreement for parents and carers 18
Appendix 3: Acceptable use agreement for KS1 pupils 19
Appendix 4: Acceptable use agreement for KS2 pupils 20
Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors 21
Appendix 6: Glossary of cyber security terminology 22

Vision Statement

Serving and celebrating our unique schools and communities, we will love, live and learn together. Valuing our pupils, staff, governors and team as people of God, we will deliver transformational learning and the flourishing of all.

Other Related Policies

- Finance Policy
- Scheme of Delegation
- Safeguarding and Child Protection Policy
- GDPR Policy
- Behaviour Policy
- Whistleblowing Policy
- Complaints Procedure

1. Introduction and Aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage 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
- Establish arrangements for identifying, reporting, responding to and escalating online-safety concerns
- Define responsibilities for filtering and monitoring systems

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our Staff HR Policies and School Behaviour Policy.

Online safety is an integral and interrelated part of the Trust's whole-school approach to safeguarding. It is reflected in relevant policies, curriculum planning, staff training, the responsibilities of the designated safeguarding lead, filtering and monitoring arrangements and engagement with parents and carers.

This policy applies to the use of school-provided and personal technology where that use affects the safety or welfare of members of the school community, the security of Trust systems or data, or the orderly operation and reputation of the school or Trust. This includes use on and off school premises.

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)
- 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
- DfE Filtering and Monitoring Standards for Schools and Colleges
- 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

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.

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 6 for a glossary of cyber security terminology.

3. Online-safety Risks

3.1 The four areas of online-safety risk

The Trust recognises that online-safety issues are broad and continually evolving. In accordance with Keeping Children Safe in Education, online risks are considered under four broad categories:

Content: exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, antisemitism, self-harm, suicide, radicalisation, extremism, extreme violence, misinformation, disinformation, conspiracy theories and content generated or manipulated using artificial intelligence.

Contact: harmful interaction with other users or with generative AI applications that simulate human interaction. This includes peer pressure, harmful advertising, grooming, exploitation, coercion and adults posing as children or young adults.

Conduct: behaviour that causes or increases the likelihood of harm, including cyberbullying, harassment, the making, sending or receiving of nudes or semi-nudes, including AI-generated or digitally altered images, and the misuse of personal information.

Commerce: risks including online gambling, inappropriate advertising, phishing, financial scams and other forms of financial exploitation.

The school's curriculum, safeguarding arrangements, acceptable-use agreements, staff training and filtering and monitoring systems will take account of all four areas.

3.2 Roles and responsibilities

Board of Directors

The Board of Directors retains strategic responsibility for online safety. It will ensure that:

- appropriate filtering and monitoring systems are in place;
- the effectiveness of filtering and monitoring is reviewed at least once every academic year;
- staff receive appropriate online-safety and filtering and monitoring training;
- online safety is reflected in the Trust's safeguarding policies, curriculum and parental engagement; and
- the Trust's arrangements do not unreasonably restrict teaching and learning through excessive blocking.

Headteacher

The Headteacher is responsible for implementing this policy within the school and for ensuring that local procedures, training, communication and record keeping are effective.

The Headteacher must ensure that:

- the relevant acceptable-use agreement is provided in an accessible and age-appropriate form to every pupil, parent or carer and member of staff, and to governors, volunteers, contractors and visitors where applicable;
- agreement is actively sought from parents or carers, pupils and staff before access to school ICT systems, networks or internet services is provided, or as soon as reasonably practicable where immediate access is operationally necessary;
- pupils are supported to understand the agreement in a manner appropriate to their age, stage of development, communication needs and any special educational needs or disabilities;
- acceptable-use expectations are explained and taught rather than relying only on the collection of a signature;
- agreements are renewed on admission or appointment, following a material change to the agreement, and at least annually;
- a secure central record is maintained showing when each agreement was issued, agreed and renewed;
- reasonable follow-up action is taken where an agreement is not returned or a person declines to agree;
- any resulting restriction of access is proportionate, based on an individual assessment and recorded; and
- a failure to sign does not adversely affect a child's safeguarding rights, statutory educational entitlement or ability to report a concern.

Designated Safeguarding Lead

The designated safeguarding lead will take lead responsibility for the safeguarding aspects of online safety and will:

- understand the filtering and monitoring systems and processes in place;
- review safeguarding alerts and concerns in accordance with the school's agreed procedures;
- support the annual filtering and monitoring review;
- ensure that online-safety concerns are appropriately recorded, assessed, escalated and referred;
- ensure that the views and needs of pupils, including vulnerable pupils and pupils with SEND, inform online-safety arrangements; and
- ensure that online safety is reflected in safeguarding training, curriculum planning and parental engagement.

4. Unacceptable Use

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

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Making, requesting, possessing or sharing digitally altered or AI-generated nude or semi-nude images of a child
- Using technology to impersonate, groom, coerce, exploit, harass or financially exploit another person
- Creating or distributing deepfakes or other manipulated content intended to harm, deceive, humiliate or intimidate
- Knowingly creating or sharing misinformation, disinformation or harmful conspiracy material
- Entering personal, special-category, confidential or commercially sensitive information into an AI tool or other online service that has not been approved by the Trust
- Using an AI tool in breach of its age restrictions, terms of use or Trust approval arrangements
- Using AI-generated output without checking its accuracy, suitability and potential bias where this could affect another person
- Presenting AI-generated work as the user's own where acknowledgement is required.
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

4.1 Exceptions from Unacceptable Use

An exception may be granted only where the proposed use has a legitimate educational, safeguarding, technical or business purpose.

Any exception must:

- be requested in advance;
- be risk assessed;
- be approved and documented by the responsible senior leader;
- include consultation with the DSL where there may be safeguarding implications;
- be limited in duration and scope; and
- be reviewed or withdrawn if circumstances change.

Technical filtering exceptions required for system administration must also be approved and recorded. No exception may permit access to illegal content or override mandatory filtering controls.

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 (staff code of conduct/disciplinary policy/behaviour policy).

5. Staff (including governors, volunteers and contractors)

5.1 Access to school ICT facilities and materials

The school's Headteacher 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 Headteacher and Primary ICT.

Requests for new or amended access must be authorised by the user's line manager or Headteacher and implemented by the ICT provider. Access must be based on the user's role and limited to what is necessary.

Access rights will be reviewed regularly and whenever a person changes role or leaves the Trust. Access for leavers will be withdrawn promptly.

5.2 Use of phones and emails

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 inform the Data Protection Officer, Leanne Noone, immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff must not use personal messaging accounts, personal cloud storage or unapproved communication platforms for school business or communication with pupils.

Staff must not use their personal devices to photograph, record or store information about pupils unless this is expressly authorised under an approved school procedure.

Staff must immediately report suspicious messages, phishing attempts, unintended disclosures and suspected account compromise in accordance with the Trust's data-breach and cyber-incident procedures.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.3 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

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

Staff should take care to follow the school's guidelines on use of social media and use of email (see section 5.2) to protect themselves online and avoid compromising their professional integrity.

5.4 Personal social media accounts

Staff use of social media, whether professional or personal and whether during or outside working hours, must be consistent with the Staff Code of Conduct and must not compromise professional boundaries, confidentiality, safeguarding responsibilities or public confidence in the Trust.

Staff must not accept or initiate social-media connections with current pupils through personal accounts. Any exceptional circumstances, such as a pre-existing family connection, must be declared to the Headteacher and managed transparently.

Staff must not post images or information that identify pupils, families or confidential school matters unless publication has been properly authorised.

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

5.5 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the ICT support provider 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, which can be found in the Staff Handbook.

Confidential work must not be undertaken where information can be overlooked, overheard or accessed by an unauthorised person. School information must not be downloaded to or stored on an unapproved personal device.

5.6 School social media accounts

The school/trust has an official Facebook/Twitter/etc. account, managed by Headteachers, central staff and administrators. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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

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

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

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

Only authorised 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

The Board of Directors is responsible for ensuring that the Trust meets the DfE filtering and monitoring standards.

Each Headteacher must nominate a member of the senior leadership team with operational responsibility for filtering and monitoring. The responsible senior leader, supported by the DSL and ICT provider, must review the effectiveness of the school's filtering and monitoring arrangements at least once every academic year and additionally when:

- a safeguarding risk or serious incident is identified;
- new technology, devices, applications or generative AI tools are introduced;
- working practices change, including remote access or bring-your-own-device arrangements;
- significant software or network changes take place; or
- the effectiveness of existing arrangements is called into question.

The review must take account of:

- the age and needs of pupils;
- pupils with SEND, communication needs or other vulnerabilities;
- the school's Prevent risk assessment;
- the devices, applications and networks in use;
- use away from school and remote access;
- generative AI and personalised or dynamically generated content;
- recent incidents and emerging risks; and
- the need to avoid unreasonable restrictions on teaching and learning.

Filtering and monitoring checks must cover all school-managed devices, relevant user groups, internet connections and school locations. A written record must identify:

- the date of the check;
- the person carrying it out;
- what was tested;
- the findings;
- required actions;
- the person responsible for each action; and
- the date of completion.

All staff must know how to report content, activity or system behaviour that causes concern. Safeguarding concerns must be reported to the DSL immediately. Technical faults must be reported to the ICT provider. A technical report does not replace a safeguarding referral.

6. Pupils

6.1 Access to ICT facilities

Computers and equipment in the school's ICT suite 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.

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 (your behaviour policy should list these items), and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Nude or semi-nude images of a child, including images that have been digitally altered or generated using artificial intelligence
- 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 headteacher / designated safeguarding lead)
- 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 the staff member in conjunction with the DSL / headteacher, 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
- Staff will not intentionally view, copy, print, forward, upload or store such an image unless viewing is unavoidable and specifically necessary to safeguard the child or report an offence. Any decision to view will be made by the DSL in accordance with current UKCIS guidance and will be recorded.
- 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 trust complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the school's 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 (including self-generated, digitally altered and AI-generated images)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

The school may respond to online behaviour outside school where it:

- poses a threat or causes harm to another pupil;
- could have repercussions for the orderly running of the school;
- adversely affects the reputation of the school or Trust; or
- involves conduct that may affect the suitability of a person to work with children.

Any response will be lawful, reasonable, proportionate and consistent with the Behaviour Policy, Child Protection Policy and Staff Code of Conduct, as applicable.

7. Parents/carers

7.1 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.

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 sign the agreement in appendix 2.

The Headteacher is responsible for ensuring that this agreement is issued, explained where necessary, actively followed up and centrally recorded in accordance with Section 3.3.

Parents and carers will be given accessible information about:

- the school's online-safety expectations;
- the nature and purpose of filtering and monitoring;
- how the school uses pupil accounts, devices and online services;
- how to report an online-safety concern; and
- sources of support for keeping children safe online.

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.

Parents and carers will also be informed, in accessible language, about the filtering and monitoring arrangements used by the school.

Where pupils are expected to use a new online service or generative AI tool, the school will consider and address:

- the educational purpose;
- applicable age restrictions;
- what personal data will be processed;
- whether a data protection impact assessment is required;
- how the provider uses and retains information;
- safeguarding and moderation arrangements; and
- the support or supervision pupils will receive.

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

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

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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.

All staff will use the password manager required by the ICT service provider to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

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

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

8.3 Data protection

All personal data must be processed and stored in accordance with the Data Protection Act 2018, UK GDPR, the Data (Use and Access) Act 2025 and the Trust's Data Protection Policy, privacy notices and retention arrangements.

Online services, applications and AI tools must be approved before they are used to process Trust information. A data protection impact assessment will be completed where processing is likely to result in a high risk to individuals.

Users must not enter personal, special-category, confidential or commercially sensitive information into a generative AI tool unless that specific use has been authorised following advice from the Data Protection Officer.

8.4 Access to facilities and materials

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

These access rights are managed by the Headteacher.

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

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 a third-party audit 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
- Critical data will be backed up in accordance with the Trust's documented backup arrangements. Backups will be appropriately secured, encrypted where necessary, separated from live systems and regularly tested to confirm that data can be restored.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT provider.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- 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 annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.
- Significant cyber incidents will be managed as potential safeguarding, data-protection and business-continuity incidents. The Headteacher, DSL, Data Protection Officer and ICT provider will be informed as appropriate.

10. Internet access

10.1 Pupils

Pupils may access school internet services only through approved accounts, devices and networks and in accordance with age-appropriate supervision and curriculum arrangements. Appropriate filtering and monitoring will apply to all pupil access.

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)
- Any other circumstances where parents/carers or visitors will be granted access to the internet.

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

10.3 Mobile phones and personal devices

The school will operate as a mobile-phone-free environment for pupils throughout the school day by default, including lessons, transitions, breaktimes and lunchtimes.

The Headteacher may authorise a proportionate exception to meet an individual pupil's medical, disability, safeguarding or other exceptional need. Any exception must be recorded and reviewed.

Detailed arrangements for possession, storage, use, confiscation and return of mobile phones and personal devices are set out in the school's Behaviour Policy or Mobile Phone Policy.

Appendix 1: Social Media Guidance for staff

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name or use a maiden name.
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

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.
- 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.
- 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

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. Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: · Be respectful towards members of staff, and the school, at all times · Be respectful of other parents/carers and children · Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: · Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way · Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident · Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
● I have read and understood the school's expectations for acceptable use and online communication. ● I understand that the school uses filtering and monitoring systems to help safeguard pupils and that no technical system can remove every online risk. ● I will support my child to follow the applicable pupil acceptable-use agreement and to report anything online that causes concern. ● I understand how to report an online-safety or safeguarding concern to the school. ● I understand that this agreement records my understanding of the school's arrangements. It does not replace the school's legal duties or make necessary safeguarding arrangements dependent upon my consent.	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for KS1 pupils

<table>
<tr><th colspan="2">Acceptable use agreement for KS1 children</th></tr>
<tr><td colspan="2">Name:</td></tr>
<tr><td colspan="2">When I use the school's ICT (like computers and equipment) and when I go on the internet. I will:
ask an adult first and make sure an adult is in the room with me
keep my passwords safe and not tell anyone except my teacher or parents
only send messages using the school's systems like TEAMS or Google Classroom, or systems that an adult in school tells me are safe
be kind and respectful when working on the computers and sending messages
never use mean or rude words when talking to other people using computers or other devices
tell an adult in school immediately if I see something that I don't like, I know is wrong, or anything that makes me feel sad
not open any attachments in emails, or click any links in emails, without checking with an adult first
not share any photos or videos of people (including me) online
carefully follow the instructions I am given by the adults in school
only use the internet to search for things I have been told to look for and that I have been told are safe
not use social media or social networking sites at school, because they are not meant for children and can be unsafe
tell an adult straight away if I see social media on a school device or if someone asks me to use it
not use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me.
I know…
I am responsible for making the right choices with technology, which will make it a useful and enjoyable tool for everyone
it is not safe to talk to people I don't know online and that I mustn't tell people my personal information like my name or where I live
school will speak with my parents if I make the wrong choices whilst using technology
to tell a teacher or a member of staff immediately if I find anything on a school computer or online that upsets me, or that I know is unkind or wrong.
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 safety rules.
I agree to follow these steps so that I learn as much as I can while using technology in school and I keep myself and others safe.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: Parent/carer agreement: I accept my child can use the school's ICT systems and internet, appropriately supervised by a member of school staff. I understand the school has a filtering system to block inappropriate websites. I accept the conditions set out above for pupils using the school's ICT systems and internet</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 4: Acceptable use agreement for KS2 pupils

Acceptable use agreement for KS2 children

Name:

When using computing equipment in school, I will:

- use computers, the internet and any technology equipment that I am given to support my learning responsibly and in the way that the adults in school ask me
- seek permission from an adult to use school equipment or access the internet and websites that have been shared with me by an adult in school and that I have been told are safe
- only use school systems to communicate safely online e.g. Teams, Google Classroom
- tell an adult straight away if I see social media on a school device or if someone asks me to use it
- always act respectfully using appropriate language when communicating online or when using technology in school
- seek the permission of an adult to search for and add images to anything I create
- always look after my own computer and online safety by creating strong passwords and keeping them safe. I will only share my password with my teacher or parents.

When using computing equipment in school, I will not:

- access social networking sites or chat rooms at school (unless my teacher has expressly allowed this as part of a learning activity)
- share any images, videos or livestreams, even if I have the consent of the person or people in the photo
- share my password with others or log in to the school's network using someone else's details
- use any personal devices from home e.g. smart phones and watches.
- view or share violent content
- open any attachments in emails, or follow any links in emails, without first checking with a teacher
- use any inappropriate language when communicating online, including in emails
- 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.

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

I will immediately let a member of staff know if I find any material which might upset, distress or harm me or others. I understand that school will speak with my parents if I do unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I accept that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I understand the school has a filtering system to block inappropriate websites. I accept the conditions set out above for pupils using the school's ICT systems and internet will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

<table>
<tr><th colspan="2">Acceptable use of the school's ICT facilities and the internet:
agreement for staff, governors, volunteers and visitors</th></tr>
<tr><td colspan="2">Name of staff member/governor/volunteer/visitor:</td></tr>
<tr><td colspan="2">When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:
Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
Use them in any way which could harm the school's reputation
Access social networking sites or chat rooms
Use any improper language when communicating online, including in emails or other messaging services
Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
Share my password with others or log in to the school's network using someone else's details
Share confidential information about the school, its pupils or staff, or other members of the community
Access, modify or share data I'm not authorised to access, modify or share
Promote any private business, unless that business is directly related to the school</td></tr>
<tr><td colspan="2">I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.</td></tr>
<tr><td>Signed (staff member/governor/volunteer/visitor):</td><td>Date:</td></tr>
</table>

Appendix 6: 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.
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.