The Key > Leaders

Mapperley Plains Primary School

ICT and Acceptable Use Policy

Non-Statutory

Approved by	Academic Committee
Original approval date	Summer 2026
Review date	Summer 2027
Version	V0.2

Inspiring learners. Shaping futures.

Contents

1. Introduction and aims....3

2. Relevant legislation and guidance....3

3. Definitions....3

4. Unacceptable use....4

5. Staff (including governors, volunteers, and contractors)....4

6. Pupils....7

7. Parents/carers....8

8. Data Security....8

9. Protection from cyber attacks....9

10. Internet access....10

11. Monitoring and review....10

12. Related policies....11

Appendix 1: EYFS and KS1 acceptable use agreement....12

Appendix 2: KS2 acceptable use agreement....13

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors....14

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

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

Misuse of IT and communication systems can damage the school and its reputation. Breaches of this policy will be addressed in line with the school's Behaviour Policy, Staff Code of Conduct and Staff Disciplinary Policy, as appropriate.
Autumn 2026 alignment update: this version retains the policy approved by the Academic Committee in Summer 2026 and aligns references and acceptable-use agreements with KCSIE 2026, the current Online Safety Policy and the Mobile Phone and Smartwatch Policy. The next scheduled review remains Summer 2027.

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Children's Wellbeing and Schools Act 2026
- Keeping Children Safe in Education 2026
- Searching, screening and confiscation: advice for schools
- Mobile phones in schools
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges

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

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 any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Entering, uploading or processing personal data about children, safeguarding information, SEND or medical information, confidential staff information or other sensitive school data in public or unapproved generative AI tools
- Using generative AI to create, alter, request or share content in a way that breaches safeguarding, behaviour, data protection, copyright or professional conduct expectations
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This list is not exhaustive. The school reserves the right to determine whether any use of ICT is unacceptable and will apply professional judgement where required.

4.1 Exceptions from unacceptable use

In exceptional circumstances, the headteacher may approve use of ICT that would otherwise be considered unacceptable, where there is a clear educational or operational need. Any such use must be agreed in advance.

4.2 Sanctions

Pupils and staff who misuse ICT may face sanctions in line with the school's Behaviour Policy, Staff Code of Conduct and Staff Disciplinary Policy, as appropriate. This may include restriction or removal of access to school ICT systems.

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

5.1 Access to school ICT facilities and materials

Access to the school's ICT systems and resources is managed by the school's ICT support provider and the Office Manager. This includes:

- Computers, tablets and other devices
- Access permissions to systems, files and applications

All staff are issued with individual login details and passwords, which must not be shared.

Staff must only access systems and information they are authorised to use. If access is incorrect or needs to be updated, this must be reported to the Office Manager or ICT support provider.

5.1.1 Use of school-supplied equipment

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

Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Update software, operating systems and applications when prompted, or as directed by the school's ICT support provider
- Connect to the school network using approved and secure methods. When using networks outside of school, staff must ensure connections are secure and avoid accessing or transmitting sensitive information on public or unsecured networks
- Report any loss, theft, damage or suspected compromise of a school device immediately to the School Business Manager, the school's ICT support provider and, where appropriate, the designated safeguarding lead or data protection officer
- Lock devices with a password when unattended. Passwords must:
  - Not be shared with others and must be changed regularly
  - Be suitably strong, in accordance with the school's password policy (see section 8.1)
  - Not be reused across multiple accounts

5.1.2 Use of phones and email

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

- This email account must be used for work purposes only
- Staff must ensure multi-factor authentication is enabled on their email account(s)
- All work-related business must be conducted using the school email account
- Staff must not share personal email addresses with parents/carers or pupils, or send work-related materials from personal accounts
- Staff must take care with the content of all email messages, as inappropriate or incorrect statements may lead to claims such as discrimination, harassment, defamation or breach of confidentiality
- Email messages may be disclosed in legal proceedings or subject access requests under the UK GDPR and Data Protection Act 2018. Deleted emails may still be recoverable and should be treated as such
- Staff must take extra care when sending sensitive or confidential information by email. Attachments must be encrypted so that information is only accessible to the intended recipient

- If an email is received in error, the sender must be informed and the email deleted. If it contains sensitive information, it must not be used or shared
- If an email is sent in error containing personal data, this must be reported immediately to the Office Manager and the school's ICT support provider, and managed in line with the school's data breach procedures

Use of Phones
• Staff must not share personal phone numbers with parents/carers or pupils
• Where staff are issued with a school phone, this must be used for all work-related communication
• School phones must not be used for personal matters
• Staff issued with mobile devices must follow the same ICT acceptable use expectations set out in section 4

5.2 Personal use

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

Personal use is permitted provided that it:
- Does not take place during teaching time or when supervising pupils
- Does not constitute 'unacceptable use' as defined in section 4
- Takes place when no pupils are present
- Does not interfere with staff duties or prevent others 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 personal use of the school's ICT facilities may fall within the scope of the school's monitoring arrangements (see section 5.5). Where breaches are identified, disciplinary action may be taken
- Staff may use personal devices (such as mobile phones or tablets) in line with the school's Mobile Phone and Smartwatch Policy

- Staff must not store any school-related data on personal devices, personal cloud storage or removable storage devices unless authorised
- Staff should be aware that personal use of ICT, even outside of school systems, can impact on their employment, for example where content is visible to pupils or parents/carers
- Staff should use email appropriately (see section 5.1.2) and take care to maintain professional standards when communicating online

5.2.1 Personal social media accounts
Staff must ensure that any use of social media, whether for personal or professional purposes, is appropriate at all times and does not bring the school into disrepute.

The school does not operate official social media accounts.

5.3 Remote access
- **The school allows staff to access ICT systems and materials remotely using secure methods.**
- **Remote access is provided through the school's VPN and approved cloud-based systems, including OneDrive**
- **Access is managed by the school's ICT support provider**
- **Staff must only use approved devices and secure connections when accessing systems remotely**
- **Staff must not access or transmit sensitive information using public or unsecured networks**
- **All data must be accessed and stored within approved systems. School data must not be downloaded to personal devices or stored outside of the school's secure environment**
- **Staff accessing ICT systems remotely must follow the same expectations as when working on site**
- **Staff must remain vigilant to security risks, including phishing, malware and unauthorised access**
- **Any concerns, breaches or suspected security incidents must be reported immediately to the Office Manager and the school's ICT support provider**
- **All information accessed remotely must be treated as confidential and handled in line with the school's Data Protection Policy**

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

To comply with Department for Education guidance and to safeguard children, the school reserves the right to filter and monitor the use of its ICT systems and network.

This may include monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity and access logs
- Other electronic communications

Only authorised personnel may monitor, access or review this information, in line with legal requirements.

The school may access email content or internet usage where necessary, including to:

- Ensure use is appropriate and in line with this policy
- Retrieve lost or deleted information
- Investigate potential misuse or breaches
- Meet legal obligations

This list is not exhaustive.

Purpose of Monitoring

The school monitors ICT use to:

- Support the safe and effective operation of systems
- Ensure compliance with school policies
- Safeguard children and staff
- Investigate concerns or incidents
- Prevent or detect misuse or criminal activity
- Meet legal obligations, including subject access and Freedom of Information requests

Roles and Responsibilities

The governing body is responsible for ensuring that:

- Appropriate filtering and monitoring systems are in place
- The school meets DfE filtering and monitoring standards
- Staff are aware of systems and trained appropriately
- Systems are regularly reviewed for effectiveness

The designated safeguarding lead (DSL) has lead responsibility for understanding filtering and monitoring systems and processes.

Staff should raise any concerns about ICT use or online activity with the DSL or the school's ICT support provider.

6. Pupils

6.1 Access to ICT facilities

- **Pupils have access to ICT facilities to support their learning. This access is provided in a safe and supervised environment.**
- **Computers and equipment in classrooms and any shared ICT areas are available to pupils under the supervision of staff**
- **Email addresses and passwords may be provided to pupils for educational purposes. Pupils must not share their passwords with others or use their accounts to access, download or share files, including software or inappropriate content, without staff permission**
- **Specialist ICT equipment, such as that used for music or design and technology, must only be used under staff supervision**
- **Pupils may be provided with access to the school's online learning platforms, which can be used in school and, where appropriate, at home to support learning**

Pupils may only use generative AI or other AI-enabled tools where a member of staff has approved the activity, the tool is appropriate for the child's age and the use is consistent with safeguarding and data protection requirements

- **Pupils must only use ICT systems in line with instructions given by staff**

6.2 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, including outside of school:

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass others, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Engaging in illegal conduct or making statements that advocate illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing nude or semi-nude images or videos, whether consensual or non-consensual
- Activity which defames or damages the reputation of the school
- Sharing confidential information about the school, other pupils or members of the school community
- Gaining or attempting to gain access to restricted systems or password-protected information without permission
- Allowing or enabling others to gain unauthorised access to the school's ICT systems
- Causing intentional damage to ICT systems or equipment
- Causing a data breach by accessing, modifying or sharing data without permission
- Using inappropriate or offensive language

Pupils may also face sanctions for inappropriate use of ICT in line with the Behaviour Policy.

7. Parents/carers

7.1 Access to ICT facilities and materials

- **Parents and carers do not have access to the school's ICT facilities as a matter of course.**
- **However, parents and carers working with the school in an official capacity, for example as a volunteer or member of the PTA, may be granted appropriate access or permitted to use school facilities at the headteacher's discretion.**
- **Where access is granted, parents and carers must abide by this policy.**

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 and carers play a vital role in modelling this behaviour for their children, particularly when communicating with the school through official channels.**
- **We ask parents and carers to sign the agreement in Appendix 1.**

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 asked to carry out.
- When pupils are asked to use websites or engage in online activity, details will be shared with parents and carers in the same way as information about homework.
- Staff will make clear, where relevant, who pupils will be interacting with online and the purpose of the interaction.
- Parents and carers may seek support and advice from the school to help ensure a safe online environment for their child.

8. Data Security

The school is responsible for ensuring appropriate security measures are in place to safeguard its systems, staff and pupils. It takes steps to protect computing resources, data and user accounts, and reviews these measures regularly.

All users of the school's ICT facilities are expected to follow safe computing practices at all times.

The school aims to meet the Department for Education's digital and technology standards for schools and colleges: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
This includes 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 must set strong passwords for their accounts and keep these secure. Passwords must not be reused across multiple platforms.
- Users are responsible for the security of their accounts and any permissions they control. Passwords must be kept confidential and changed regularly.
- Staff and pupils who share account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights removed.
- All staff must use the password manager provided or approved by the school's ICT support provider to store passwords securely. Where passwords are issued to pupils, these will be generated by staff and stored securely in case they need to be reset.

8.2 Software updates, firewalls and anti-virus software

- All school ICT devices that support software updates, security updates and anti-virus protection will have these installed and configured to update regularly or automatically.
- Users must not delete, modify or interfere with systems, software, data or information.
- Users must not download or install software from external sources without authorisation from the school's ICT support provider.
- Users must not attempt to bypass or undermine any security measures in place to protect the school's systems or data.
- Any incoming files must be virus-checked before they are opened or downloaded.
- Any personal devices connected to the school's network must meet the same security standards.

8.3 Data protection

- All personal data must be processed and stored in line with data protection legislation and the school's Data Protection Policy.
- The Data Protection Policy is available on the school website.

8.4 Access to facilities and materials

- All users of the school's ICT facilities will have clearly defined access rights to systems, files and devices.
- These access rights are managed by the school's ICT support provider and Office Manager.
- Users must not access, or attempt to access, systems, files or devices for which they do not have permission. If access is provided in error, or information is shared inappropriately, this must be reported immediately to the Office Manager or the school's ICT support provider.
- Users must log out of systems and lock devices when not in use to prevent unauthorised access. All equipment and systems should be logged out of and shut down at the end of each working day.

8.5 Encryption

- The school ensures that its devices and systems have an appropriate level of encryption.
- Staff may only use personal devices (including computers and USB drives) to access school data, work remotely or take personal data off site where they have been specifically authorised to do so by the headteacher.
- Such use will only be permitted where devices meet the security and encryption standards set by the school's ICT support provider.

9. Protection from cyber attacks

The school will take proportionate steps to prevent, detect and respond to cyber attacks and security incidents. The school will:

- Work with governors and the ICT support provider to ensure cyber security is appropriately resourced and prioritised
- Provide regular training for staff, including as part of induction, covering key areas such as phishing, password security, safe use of devices, data protection and how to report incidents
- Ensure staff are aware of procedures for reporting and responding to cyber security incidents
- Regularly review whether systems and software require updating or replacement to maintain security
- Not engage in ransom demands in the event of a ransomware attack
- Put controls in place that are:
  - o Proportionate, supported by external review where appropriate (e.g. 360 Safe)
  - o Multi-layered, with clear expectations for all users
  - o Up to date, with systems in place to monitor required updates
  - o Regularly reviewed and tested to ensure effectiveness
- Back up critical data regularly and store backups securely using approved cloud-based systems
- Ensure responsibility for the security of core systems, including the MIS, sits with the ICT support provider
- Ensure staff:
  - o Use a VPN when accessing systems remotely
  - o Enable multi-factor authentication where available
  - o Store passwords securely using an approved password manager
- Ensure regular access reviews are carried out so that users have appropriate permissions
- Ensure firewalls and other security systems are in place and active across the network
- Ensure appropriate cyber security measures are in place to detect and respond to threats
- Check that suppliers meet appropriate security standards, such as Cyber Essentials certification
- Maintain and test an incident response plan, including communication procedures and reporting requirements (including reporting to Action Fraud where necessary)
- Work with the Local Authority to access advice and support on cyber security where appropriate
- Conduct a cyber risk assessment annually, and review this following any significant incident
- Ensure senior leadership oversight of cyber security and risk

10. Internet access

- The school's wireless internet connection is secure and monitored.
- The school uses filtering systems to restrict access to inappropriate content. While these systems are robust, they are not foolproof.
- Separate access arrangements are in place for staff and pupils. Access for visitors is only provided where authorised.
- Any concerns about inappropriate content, or sites that have been incorrectly blocked, should be reported to the Office Manager or the school's ICT support provider.

10.1 Pupils

Pupils have access to the school's Wi-Fi network to support teaching and learning.

- Wi-Fi access is available on school devices and within supervised areas of the school
- Access is filtered and monitored to restrict inappropriate content
- Pupils may only use Wi-Fi under the supervision of staff and for educational purposes
- Pupils do not independently request access; this is managed by staff as part of teaching and learning
- Use of Wi-Fi is limited to activities directed or approved by staff

10.2 Parents/carers and visitors

Parents, carers and visitors will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

Authorisation may be granted where:

- Parents or carers are working with the school in an official capacity, for example as a volunteer or member of the PTA
- Visitors require access to fulfil the purpose of their visit, for example to support a presentation or professional work
- Staff must not share Wi-Fi access details with anyone who is not authorised. Failure to follow this may result in disciplinary action.

11. Monitoring and review

- The headteacher, supported by the Office Manager and the school's ICT support provider, is responsible for monitoring the implementation of this policy and ensuring it remains up to date.
- This policy will be reviewed annually, or sooner if required by changes to legislation, safeguarding guidance, technology or the school's systems. The next scheduled review is Summer 2027.
- The governing body is responsible for approving this policy and overseeing its effectiveness.

12. Related policies

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

- Online Safety Policy (including AI safeguarding and use expectations)
- Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Staff Disciplinary Policy
- Data Protection Policy
- Remote Education Policy
- Mobile Phone and Smartwatch Policy

Appendix 1: EYFS and KS1 acceptable use agreement

This agreement is written in child-friendly language. Staff should explain it at an appropriate level and parents/carers should support the expectations at home.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET

Name of child: _____

When I use school computers, tablets or the internet, I will:

- ask a teacher or adult before I use them
- only use websites and AI tools that a teacher or adult has told me I can use, and use them in the way I have been shown
- tell an adult straight away if I open something by mistake, receive a message from someone I do not know or see anything that worries, upsets or harms me or someone else
- use school devices for learning and schoolwork
- be kind and respectful to other people
- look after school devices and report anything that is broken or not working
- use only my own username and password and keep my password private
- keep personal information private unless a trusted adult says it is safe to share
- save my work where my teacher tells me to
- log off or shut down when I have finished.

Signed (child)	Date

Parent/carer agreement: I support these expectations and will help my child understand how to use the school's ICT systems, internet and approved AI tools safely and responsibly.

Signed (parent/carer)	Date

Appendix 2: KS2 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS, INTERNET AND AI

Name of child: _____

When I use the school's ICT systems and internet, I will:

- use them responsibly and for educational purposes
- only use systems, websites and online services when a member of staff has allowed me to
- keep usernames and passwords private and never use somebody else's account
- keep personal information private unless a trusted adult has agreed it is safe to share
- tell an adult immediately if I see or receive anything that could upset, distress or harm me or another person
- only use AI tools when a member of staff has approved the activity and explained how I should use them
- log off or shut down devices properly when I have finished.

I will not:

- access social media, chat rooms, gaming sites or other restricted services unless a teacher has explicitly approved this as part of learning
- open unknown links or attachments without checking with a member of staff
- use abusive, threatening, discriminatory, sexualised or otherwise inappropriate language online
- create, request, link to, share or post pornographic, offensive, obscene, sexualised or harmful material, including material created or altered using AI
- attempt to bypass filtering or monitoring systems
- arrange to meet someone I only know online without first telling a parent/carer or another trusted adult.

Personal mobile phones and smartwatches

If I have permission to bring a phone or communication-enabled smartwatch to school, I understand that Mapperley Plains is a mobile phone-free school. I will follow the school's hand-in and collection procedure and will not access or use the device at any point during the school day unless the Headteacher has authorised an individual exception.

Signed (child)	Date

Parent/carer agreement: I support these expectations, including the school's mobile phone-free arrangements, and will help my child understand them.

Signed (parent/carer)	Date

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

Name: _____ Role: _____

When using the school's ICT systems, internet, cloud services or school devices, I will:

- use systems for legitimate educational or school-business purposes appropriate to my role, with only the limited occasional personal use permitted by section 5.2 of this policy
- follow safeguarding, data protection, information security and professional conduct requirements
- keep passwords and authentication details secure and never use another person's account
- use school-approved systems for storing, processing and sharing school information
- report online safety concerns, suspected data breaches, security incidents and filtering or monitoring failures promptly
- take reasonable steps to keep school devices physically secure and locked when unattended
- use generative AI only in accordance with the Online Safety Policy, this policy and any school instructions.

I will not:

- access, create, store, share or send illegal, pornographic, violent or otherwise inappropriate material except where specifically required and authorised for safeguarding or legal purposes
- use school systems in a way that could undermine safeguarding, security or the professional reputation of the school
- install unauthorised software or connect unauthorised hardware or devices
- attempt to bypass or disable security, filtering or monitoring controls
- input, upload or process personal data about children, safeguarding information, SEND or medical information, confidential staff information or other sensitive school data in public or unapproved generative AI tools
- take or share images of children except in accordance with school policy and authorisation
- access, modify or share information I am not authorised to access.

Signed	Date