ABINGDON

Policy Index

At a Glance - Policy Summary
1. Introduction
2. General Principles
3. Use of School IT Systems and Equipment
4. Communication and Internet Use
5. Mobile Devices and Remote Access
6. Privacy Expectations and System Monitoring

At a Glance - Policy Summary

This policy outlines the acceptable use of Abingdon Foundation's (Abingdon Senior School, Abingdon Prep School and Abingdon School Enterprises Limited) ICT resources. The Foundation is committed to using ICT to develop its educational provision and resources for all its students and staff. We encourage everyone in the Foundation to make use of all the ICT opportunities that are available whilst following the advice and guidance set out in this policy. All staff (including governors, volunteers, self-employed staff and casual staff) must adhere to these guidelines. A summary of the key “points to remember” is below:

A. Purpose & Professionalism

Use IT resources primarily for professional duties, maintaining responsible and ethical conduct at all times. All electronic interactions should uphold the school's reputation and values.

B. Security is Mandatory

Use only your strong, unique passwords (at least 12 characters) and multi-factor authentication where available. Never share account credentials and lock devices when unattended. Report security concerns immediately to the IT Department. Keep software up-to-date and only use administrator accounts when specifically needed for authorised tasks. Be vigilant against phishing attempts and never connect unknown USB devices.

C. Safeguarding Students

Protecting students online is paramount. Report any online safety concerns regarding students immediately to the Designated Safeguarding Lead. Maintain professional boundaries in all online interactions with students, using only official school channels. Never connect with current students or recent former students (within three years) on personal

social media. Comply with the Taking, Storing and Using Images of Children Policy when capturing or sharing pupil images.

D. Data Protection

Handle personal and sensitive data according to the school's Data Protection Policy. Avoid storing sensitive school data on personal devices unless absolutely necessary and authorised in advance by your line manager. Transfer any pupil images taken on personal devices to school systems promptly and delete them from personal devices. Dispose of sensitive printed data securely using designated confidential waste facilities.

E. Personal Use

Limited, brief personal use of school IT is permitted if it doesn't interfere with work, incur costs, or violate policy. Using school IT for personal business or gain is prohibited.

F. Prohibited Activities

Do not access or attempt to access, create, or share illegal, obscene, indecent, or extremist material. Avoid copyright infringement, attempts to bypass security/filtering systems, cyberbullying, and using IT for illegal activities. Don't install unauthorised software, click on suspicious links, or create malicious AI-generated content including deepfakes. Using VPN services without prior approval from the IT department is not permitted.

G. Personal Devices (BYOD)

Secure personal devices used for work with password/biometric protection, encryption, and current security updates. Follow the Personal Device Security Checklist before accessing school systems. Be aware that using personal mobile data (4G/5G) on school grounds bypasses school filtering, but this policy still applies to all online activity. While general web browsing on BYOD networks isn't routinely stored, attempts to access blocked sites are logged.

H. Reporting

You must report policy violations appropriately: safeguarding concerns about students to the DSL, concerns about staff conduct to the Head, security incidents to IT, and general misuse concerns to IT or HR. Proactively use the Self-Disclosure form for accidental access to inappropriate content to maintain transparency and avoid misunderstandings during routine monitoring.

I. Monitoring

All use of school IT systems may be monitored for security, compliance, and safeguarding purposes. Staff should have a limited expectation of privacy when using school-owned systems and networks. The school may access user data and devices for system maintenance, investigation of policy violations, or legal compliance, with authorisation from the IT Director or a member of the Senior Leadership Team.

J. Training

Cybersecurity and IT training is a critical component of the Foundation's security protocols.

Completion of all assigned cybersecurity awareness or IT training is mandatory for all staff. This requirement protects school data, systems, and the wider school community from cyber threats.

This introduction serves as a quick reference. You are required to read and comply with the full ICT Acceptable Use & Online E-Safety Policy (below).

IT Director and Designated Safeguarding Lead
Last Internal Policy Review: May 2026
Last Governor Review: May 2026
Next Governor Review: May 2027

1. Introduction

The Director of IT owns and maintains this policy in collaboration with the Designated Safeguarding Lead (DSL) and the Senior Leadership Team (SLT). The policy is reviewed annually by its owners and the Governors, or more frequently as needed, to ensure it remains current with technological advancements and evolving regulatory requirements.

Key Contacts:

- Director of IT - Niki Dinsey, niki.dinsey@abingdon.org.uk
    - For technical queries, system access issues, and general IT support
- Deputy Head Pastoral & Designated Safeguarding Lead - Helen Keevil, helen.keevil@abingdon.org.uk
    - For all safeguarding concerns related to online activity
    - For general queries about policy application in pastoral contexts
- Compliance Officer - Amy Hadden, amy.hadden@abingdon.org.uk
    - For data protection concerns, including accidental data sharing incidents
    - For questions about compliance with this policy and related regulations
- IT Service Desk - x266, support.it@abingdon.org.uk
    - For day-to-day technical support and minor issues
- Director of Finance and Operations - Justin Hodges, justin.hodges@abingdon.org.uk
    - For queries relating to data management and operational aspects of IT systems

1.1 Purpose and scope of the policy

This ICT and E-Safety Policy (Acceptable Use Policy) outlines the standards and practices expected of all Abingdon Foundation staff members, comprising Abingdon Preparatory School, Abingdon Senior School and Abingdon School Enterprises when using the school's IT systems and equipment. It aims to ensure that IT resources are used safely, securely, and in compliance with relevant laws and regulations.

This policy applies to:

- All staff members, including teaching staff, support staff, casual workers, volunteers and self-employed staff
- Any visitors using Abingdon Foundation digital equipment or resources also fall under this policy for the relevant period.
- All IT systems and equipment provided by Abingdon School
- Use of personal devices when accessing school systems or conducting school business
- Both on-site and remote use of school IT resources

1.2 Definitions of key terms

For the purposes of this policy:

- ***"ICT"*** refers to information and communications technology, which includes all computer hardware, software, networks, and electronic communication systems provided by the school.
- ***"Users"*** refers to all staff members and other individuals granted access to the school's IT resources.
- ***"Personal data"*** means any information relating to an identifiable person as defined by current data protection legislation. This includes any special category personal data as defined in data protection legislation.
- ***"Sensitive data"*** includes personal data and any information deemed confidential by the school.
- ***"School-owned devices"*** refers to any computing device owned by the school, regardless of location in use.
- ***"Personal devices"*** refers to any computing device owned by staff or students that connects to the Foundation's BYOD Wi-Fi networks.

1.3 Policy Objectives

The objectives of this policy are to:

- Protect the school's IT resources from misuse and security threats
- Safeguard personal and sensitive data processed by the school
- Safeguard students' well-being
- Enable the DSL and their team to actively monitor and report on IT use
- Ensure compliance with relevant laws and regulations
- Promote responsible and professional use of IT resources
- Protect the reputation of Abingdon School

1.4 Related Policies and Procedures

This policy should be read in conjunction with other relevant school policies, including but not limited to:

- Data Protection Policy
- Safeguarding Policy
- Staff Code of Conduct
- Social Media Policy
- Taking, Storing and Using Images of Children Policy
- Equal Opportunities Policy
- Staff AI Guidance
- Staff Disciplinary Policy

1.5 Compliance

All use of IT resources must comply with relevant UK legislation and statutory guidance, including but not limited to:

Legislation:

- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Communications Act 2003
- Equality Act 2010
- Data Protection Act 2018

Statutory Guidance:

- Keeping Children Safe in Education (KCSIE) (DfE)
- Meeting Digital and Technology Standards in Schools and Colleges (DfE)

2. General Principles

2.1 Acceptable Use Overview

Users of Abingdon School's IT resources are expected to:

- Use these resources primarily for purposes related to their professional duties
- Act responsibly and ethically at all times
- Respect the rights and privacy of others
- Protect the integrity and security of the Foundation's systems and data

Legal, Decent, Honest: Anything created, stored, sent or processed using IT must be socially and legally acceptable. Users must not use IT resources for any illegal activities, including but not limited to:

- Accessing, creating, or transmitting material that is obscene, indecent, or pornographic
- Infringing copyright or intellectual property rights
- Hacking or attempting to breach system security
- Sending malicious or threatening communications
- Accessing or sharing materials that may encourage radicalisation, support or promote terrorism, or compromise counter-terrorism measures

2.2 Professional Conduct Expectations

When using IT resources, staff are expected to:

- Maintain high standards of conduct in line with the Staff Code of Conduct, school policies, training and relevant professional standards
- Uphold the reputation and values of Abingdon School
- Communicate professionally and courteously in all electronic interactions
- Respect the principles of diversity, equity and inclusion, including the Equality Act 2010 and the School's Equal Opportunities Policy
- Be mindful of the potential impact and permanence of electronic communications

2.3 Safeguarding and Prevent Duty

In accordance with Abingdon's Safeguarding Policy and KCSIE, all users have a duty to protect students from online risks, including radicalisation, sexual exploitation, and cyber-bullying. Any concerns regarding online safety or inappropriate use of IT must be reported to the Designated Safeguarding Lead immediately.

Staff must:

- Be aware of and comply with the school's safeguarding policies and Staff Code of Conduct when using IT resources
- Report any concerns about pupils' online safety, inappropriate content, or potential radicalisation through online channels to the Designated Safeguarding Lead
- Report any concerns about a staff member's online conduct or use of IT resources directly to the Head, in line with the procedures outlined in the school's Safeguarding Policy
- Exercise caution, professional judgment, and appropriate professional boundaries in all online interactions with students

2.4 Reporting Inappropriate Behaviour

Staff members have a responsibility to report on discovery of any observed behaviour that contravenes this policy, raises safeguarding concerns, or involves the misuse of ICT resources. Prompt reporting is crucial for maintaining a safe and secure digital environment.

2.4.1 Defining Inappropriate Behaviour

In the context of ICT use, inappropriate behaviour includes, but is not limited to:

- Accessing, creating, downloading, or transmitting material that is illegal, obscene, indecent, offensive, pornographic, or promotes extremism or terrorism
- Engaging in or facilitating cyberbullying, harassment, or sending malicious/threatening communications
- Infringing copyright or intellectual property rights (e.g., illegal software downloads, unauthorised sharing of licensed materials)
- Attempting to breach or circumvent system security measures, including hacking or unauthorised access
- Sharing account passwords or using another individual's login credentials.

- Using school ICT resources for significant personal gain, running a personal business, or activities that interfere with professional duties
- Any breach of the school's Safeguarding Policy, Staff Code of Conduct, Data Protection Policy, or other related policies through the use of ICT
- Connecting unauthorised or potentially harmful devices or software to the school network

Inappropriate use of School IT equipment or networks will be dealt with under the School's Disciplinary Policy and could result in dismissal.

2.4.2 Reporting Channels

The appropriate channel for reporting depends on the nature of the concern:

- Any concerns related to the potential safeguarding or welfare of a pupil arising from ICT use (e.g., exposure to harmful content, cyberbullying, inappropriate contact, radicalisation concerns) must be reported immediately and directly to the Designated Safeguarding Lead, following the procedures outlined in the school's Safeguarding Policy
- Concerns regarding the conduct of another staff member in relation to ICT use that may constitute a safeguarding risk or breach the Staff Code of Conduct should be reported directly to the Head, in line with the procedures outlined in the school's Safeguarding Policy and Staff Code of Conduct
- Staff who are aware of suspected security incidents (e.g., phishing attempts, malware, unauthorised access, data breaches) or general misuse of ICT resources not related to immediate safeguarding risks should report their findings promptly to the IT Department. You may also report general misuse concerns to the HR Department
- Staff who inadvertently access inappropriate content or trigger web blocks are encouraged to use the Self-Disclosure of Potential IT Concerns form proactively

2.4.3 Reporting Process

When making a report, please provide as much detail as possible to facilitate the investigation. This should ideally include:

- Date and time of the incident or observation
- Location or specific system/platform involved (if applicable)
- Individuals involved (if known)
- A clear description of the behaviour or incident observed
- Any relevant evidence (e.g., screenshots, URLs, email details – handled appropriately according to data protection principles)

All reports will be treated seriously and investigated appropriately, respecting confidentiality as far as possible within the constraints of a thorough investigation and any legal or safeguarding requirements.

2.5 Efficient and Sustainable Use

Users should:

- Use IT resources efficiently and avoid unnecessary waste (e.g., excessive printing)
- Be mindful of the environmental impact of technology use
- Report faulty equipment promptly to the IT department for repair or replacement

2.6 Continuous Learning and Development

Staff have a duty to perform mandatory IT and Cyber Security awareness training when requested and are encouraged to:

- Keep their ICT skills up-to-date
- Engage with training opportunities provided by the school
- Stay informed about emerging digital risks and best practices for online safety

Cybersecurity training is a critical component of the Foundation's security protocols. Completion of all assigned cybersecurity awareness training is mandatory for all staff. This requirement protects school data, systems, and the wider school community from cyber threats.

2.7 Parental Communication and Engagement in Online Safety

Recognising the vital role parents play in promoting online safety, the Foundation is committed to fostering a collaborative partnership to protect pupils. Staff are expected to support and contribute to the school's initiatives for parental engagement as appropriate.

The school will facilitate this partnership through:

- Utilising established channels such as Weekly Mailings, School Websites and the parent/community portal to share relevant information, advice, and updates regarding online safety expectations and emerging risks
- Providing opportunities for parents/guardians to enhance their understanding of online safety through webinars, information evenings, or signposting to expert resources
- Ensuring parents are aware of the school's approach to online safety and the relevant sections of the Student ICT Acceptable Use Policy

Staff should direct parental queries regarding online safety resources or school initiatives to the appropriate contact person, typically the Designated Safeguarding Lead or relevant pastoral staff.

3. Use of School IT Systems and Equipment

3.1 Access and Security

3.1.1 User Accounts and Passwords

- Staff must use only their own account credentials to access school systems
- Sharing of accounts or passwords is strictly prohibited
- Passwords must meet the following minimum requirements:
    - At least 12 characters in length (longer is better)
    - Consider using passphrases - memorable sequences of words (e.g., "correct-horse-battery-staple")
    - Include a mix of uppercase and lowercase letters, numbers and symbols
    - Avoid singular, easily guessable information (names, dates, dictionary words)
    - Each password must be unique across different systems and applications
- Password Management:
    - We strongly recommend the use of a reputable password manager (such as LastPass, Bitwarden, 1Password, or similar NCSC-approved solutions)
    - Browser password saving features may be used for non-sensitive accounts only, provided that:
        - The device is secured with strong authentication
        - The browser's sync feature is either disabled or properly secured with a strong passphrase
        - The device is not shared with other users
- Multi-factor authentication (2FA/MFA) must be enabled for all accounts where available, particularly for email, cloud storage, and administrative systems
- Password reset procedures must be followed promptly when requested by IT
- Report any suspected password compromise immediately to the IT Department
- Staff must lock devices when leaving them unattended, even briefly
- Automatic screen locking must be enabled on all devices after a few minutes of inactivity

Administrator Account Usage:

- Staff members granted administrator-level privileges must adhere strictly to the principle of least privilege to minimise security risks
- Standard user accounts must be used for all routine daily tasks, including email, web browsing, and document processing
- Administrator accounts should only be logged into when specific administrative tasks requiring elevated privileges are necessary. Staff must log out of administrator accounts immediately after completing the necessary administrative tasks and revert to using their standard user account
- Elevated privileges must not be used for day-to-day activities due to the increased security risks involved

3.1.2 System and Network Security

- Users must not attempt to circumvent or disable security measures
- The IT department must approve the installation of software on school devices
- Staff should be vigilant against phishing and other cyber threats
- Any suspected security breaches must be reported immediately to the IT department

3.1.3 Cybersecurity Measures

- All school-owned devices must have up-to-date antivirus software installed and regularly updated
- Staff must ensure that software and operating systems on their devices are kept up-to-date with the latest security patches; don't put it off
- Use of personal devices to access school systems must comply with 5.1 Use of Personal Devices (BYOD)
- Staff must use caution when connecting to public Wi-Fi networks
- Email attachments from unknown or suspicious sources should not be opened
- Staff should be wary of unexpected requests for personal or financial information, even if they appear to come from known sources
- The use of USB devices and other removable media is strongly discouraged due to significant security risks. Staff should:
    - Use cloud storage (Google Drive) for files where possible
    - Only use USB drives when it is absolutely necessary (please check with IT before doing so)
    - Always scan removable media for viruses before connecting
    - Never use unknown, found, or gifted USB devices under any circumstances
    - Report any suspicious USB device found on school premises to IT
- Staff must not attempt to disable or bypass the school's firewall or other security measures
- Make regular backups of important data (contact IT if unsure of how to do this)
- Use Google Drive where at all possible
- Staff should report any suspected malware infection or unusual system behaviour to the IT department immediately

3.1.4 Cyber Incident Reporting

- Staff must report any suspected data breaches or security incidents to the IT department and the Compliance Officer without delay
- In the event of a ransomware attack or other serious cyber incident, staff should disconnect the affected device from the network and seek immediate assistance from the IT department

3.2 Personal use

3.2.1 Limited Personal Use

Reasonable personal use of school IT resources is permitted, provided it:

- Does not interfere with work duties
- Is kept to a minimum
- Does not incur additional costs to the school
- Complies with this policy and other relevant school policies, particularly the Staff Code of Conduct policy

While 'reasonable personal use' is permitted, it should remain brief and infrequent, ensuring it never takes precedence over professional responsibilities. Examples of generally acceptable personal use include quickly checking a personal email account during a break, brief online banking, or checking transport schedules.

3.2.2 Prohibited Personal Use

School IT resources must not be used for:

- Running a personal business or for personal gain
- Accessing inappropriate content
- Any illegal activities
- Any activity that could bring the school into disrepute

Examples of use considered unacceptable would include more than minimal time spent on personal social media, streaming non-work-related videos during work hours, engaging in online gaming, running a personal business, or any activity that consumes significant network resources or contravenes other sections of this or other School policies.

3.3 Software and Licensing

3.3.1 Authorised Software

- Only software licensed and approved by the school may be installed on school devices
- Staff must comply with all software licensing agreements

3.3.2 Prohibited Software and Activities

The following software and activities are strictly prohibited on school systems and devices:

- Peer-to-peer file-sharing software
- Software that attempts to bypass school security measures
- Virtual Private Networks (VPN) without prior authorisation
- Any software that could potentially harm the school's systems
- Cryptocurrency mining, software or activities

- Software for distributed computing projects without prior authorisation

3.4 Data protection and confidentiality

Staff handling of personal data, confidentiality and data protection must comply with the school's Data Protection Policy.

3.5 Equipment Care and Use

3.5.1 Care of Equipment

- Staff are responsible for taking reasonable care of the school's IT equipment assigned to them
- Staff must report any damage or loss promptly to the IT department
    - The IT department will assess any damaged equipment and determine whether repair or replacement is necessary
    - In cases of significant damage or loss, IT will report the incident to either the Director of Finance and Operations for Support Staff or the Deputy Head Academic for Teaching Staff
    - Staff may be held responsible for damage caused by negligence or misuse
- When transporting school equipment off-site, staff must ensure it is securely stored and not left unattended in vehicles

3.5.2 Return of Equipment

- Upon leaving employment or on demand, staff are responsible for the return of all school-owned equipment to the IT department
- Failure to return equipment may result in legal action by the School
- Teaching staff leaving in the summer must return their equipment at the end of the summer term
    - If you require access to a device for the remainder of your employment, IT can provide a Chromebook to be returned by the end of August

3.5.3 Removal of Non-Portable Equipment

- Staff must not remove non-portable digital and electronic equipment (such as desktop computers, monitors, printers, etc.)from school premises without prior permission from the IT Director
- Requests to remove such equipment must include a clear business justification, expected duration of removal, and confirmation of appropriate security measures during transport and off-site storage
- Staff members are responsible for the security, safe transport, and return of any non-portable equipment they are authorised to remove
- All equipment removal must be appropriately documented, including condition at removal and return
- The IT Department maintains a register of all equipment removed from school premises

3.6 Sustainable ICT Practices and Resource Use

In alignment with the Foundation's values and commitment to environmental responsibility, all users are expected to employ sustainable practices when using ICT resources. This includes minimising waste, conserving energy, and using equipment efficiently.

3.6.1 Promote Digital Alternatives

Staff are encouraged to prioritise digital methods for communication, note-taking, document sharing, and collaboration to reduce reliance on printing. Utilise school-provided platforms like Google Workspace (Docs, Sheets, Drive) or Showbie wherever feasible.

3.6.2 Efficient and Mindful Printing

Evaluate the necessity of printing documents; consider if a digital copy suffices.

- Staff should minimise printing where possible. Avoid printing emails unless necessary
- Default to double-sided (duplex) and black and white printing settings whenever appropriate, particularly for drafts or internal documents. Staff are encouraged to adjust their default printer settings accordingly; guidance is available from the IT Service Desk
- Avoid printing lengthy documents, presentations, or full email threads unless essential for accessibility or specific pedagogical requirements
- Direct bulk printing requirements through the high-volume ‘Canon’ multi-function devices.
- Personal printing should be kept to a minimum and may be subject to charges

3.6.3 Secure Printing and Document Disposal

Be mindful of where printed materials will emerge and ensure sensitive or confidential information is not left unattended at printers.

- Utilise Canon devices' secure print release features via PaperCut for confidential documents
- Dispose of printed documents containing sensitive or personal data securely to prevent unauthorised access and ensure compliance with the Data Protection Policy
- Use designated confidential waste bins or shredders as appropriate
- Consult the Data Protection Policy or Compliance Officer for specific guidance

3.6.4 Energy Conservation

Actively reduce energy consumption associated with ICT equipment:

- Power down monitors when leaving your workspace for extended periods or at the end of the day
- Ensure computers and laptops are configured to use power-saving modes during periods of inactivity

- Shut down computers at the end of the working day unless required for updates or specific tasks
- Report faulty equipment promptly to the IT department, as malfunctioning equipment can consume excess energy

3.6.5 Print Monitoring

- The school employs print management software (PaperCut) to monitor and account for user and departmental printing
- IT, Finance, and the DFO review copier usage at regular intervals. Users may be required to justify excessive printing levels
- The primary aim of print management is to reduce waste and encourage responsible, sustainable use of resources

4. Communication and Internet Use

4.1 Email Use

4.1.1 Professional Communication

- Staff should use school email accounts for all formal work-related communication
- Emails should be composed with the same care and professionalism as formal letters
- Staff should be aware that emails may be subject to disclosure under GDPR Subject Access Requests (SAR)

4.1.2 Email Etiquette

- Use clear, concise language and an appropriate tone
- Check recipients carefully before sending, especially when using 'Reply All.'
- Use the 'Bcc' field to protect privacy when sending to multiple external recipients

4.1.3 Email Security

- Exercise caution with email attachments, particularly from unknown sources
- Do not open suspicious links or attachments
- Report any suspected phishing attempts to the IT department immediately

Signs of potentially malicious emails:

- Unexpected or unsolicited emails, especially those claiming to be from official sources
- Emails that create a sense of urgency or demand immediate action
- Poor grammar, spelling errors, or unusual phrasing
- Generic greetings (e.g., "Dear Sir/Madam") instead of personalised ones
- Email addresses that don't match the purported sender's organisation
- Requests for personal information, login credentials, or financial details
- Unexpected attachments, particularly executable files (.exe, .scr, .zip)

- Links that don't match the stated destination when hovering over them
- Threats or unusual promises (e.g., account suspension, unexpected winnings)

Best practice:

- Verify unexpected requests through a separate, known channel (e.g., phone call)
- Check the full email address of the sender, not just the display name
- Be wary of emails asking you to log into accounts via provided links
- If unsure, contact the IT department before taking any action

Remember:

- The school will never ask for your password
- Be particularly vigilant when accessing emails on mobile devices
- If you think you've fallen for a phishing attempt, immediately notify the IT department

4.1.4 Personal Use of Email

- Personal use of school email must adhere to the conditions outlined in Section 3.2 Personal Use

4.2 Internet Use

4.2.1 Acceptable Internet Use

- Internet access is provided primarily for work-related purposes
- Any personal internet use must adhere to the conditions outlined in Section 3.2 Personal Use
- Staff may connect personal devices to the provided Staff BYOD network. See section 5.1 Use of Personal Devices (BYOD)

4.2.2 Prohibited Internet Use

- Accessing, creating, or transmitting material that is illegal, offensive, or inappropriate
- Downloading large files that may impact network performance
- Assessing premium live-broadcast sporting events, like Football, Boxing or F1, via illegal streaming services
- Peer-to-peer file sharing. Torrents or other services
- Using Tor to access '.onion' sites or the Dark Web
- Use of VPN services to circumvent the school's firewall, filtering and monitoring without prior approval from the IT department
- Using the internet in any way that could bring the school into disrepute

4.2.3 Streaming Media

- Streaming of audio or video for work purposes is permitted

- Personal streaming should be limited and not interfere with work duties or network performance

4.3 Social Media Guidelines

4.3.1 Professional Use of Social Media

- Staff using social media on behalf of the school must adhere to the school's Social Media Policy

4.3.2 Personal Use of Social Media

- Staff should be mindful of their professional reputation when using personal social media
- Do not identify yourself as a representative of the school on personal accounts without permission
- Do not share confidential school information on personal social media
- Ensure that your privacy settings on personal social media accounts are appropriately secure
- Be aware that your online behaviour, even on personal accounts, can impact your professional role

4.3.3 Social Interaction with Students on Social Media

- Staff must not communicate with current students (or those who have left the School in the last three years) via personal social media accounts
- Any social media interaction with students must be through official school channels and for educational purposes only
- Staff should not request or accept requests to "friend" or "follow" current pupils (or those who have left the School in the last three years) on personal social media accounts
- If a staff member receives contact from a pupil on social media:
    - They should decline the contact
    - Explain the safeguarding reasons for this decision
    - Notify the Designated Safeguarding Lead
    - If there are genuine reasons for this type of communication (e.g., clubs managed outside of work), this should be discussed with and approved by the DSL
- Staff should immediately report to the Head Teacher any instance of their social media account being used without authorisation to impersonate them, misrepresent them, or portray them inaccurately

4.3.4 Reporting Concerns

- If staff become aware of inappropriate or potentially harmful social media activity involving students, they should report this to the Designated Safeguarding Lead immediately

- Staff should be aware of and follow the school's procedures for reporting online safety concerns

4.4 Instant Messaging and Video Conferencing

4.4.1 Approved Platforms

- Use only school-approved platforms for instant messaging and video conferencing. These include: Google Chat, Google Meet, Slack, Zoom
- Ensure appropriate security settings are in place for online meetings

4.4.2 Professional Conduct

- Maintain professional standards in all online interactions, including dress code and background environment for video calls
- Be aware of confidentiality and data protection when sharing screens or documents

4.4.3 Monitoring and Reporting

- Be aware that all instant messages and video conferences conducted on school platforms may be monitored and logged for safeguarding and security purposes
- The school reserves the right to access, review, and use the content of instant messages and video conferences in the course of disciplinary proceedings or investigations
- Report any inappropriate or concerning content or behaviour in instant messaging or video conferencing to the DSL or the IT department immediately

4.4.4 Data Protection and Privacy

- Instant messages are subject to Data Protection regulations, including GDPR
- These communications may be disclosable under Subject Access Requests (SARs) or Freedom of Information (FOI) requests
- Avoid sharing personal or sensitive information about students or staff through instant messaging unless absolutely necessary and through approved, secure channels
- Be mindful that even 'deleted' messages may be recoverable and subject to disclosure

4.4.5 Best Practice

- Use school accounts, not personal accounts, for all school-related communications
- Be cautious about who you add to group chats or video calls, ensuring all participants have a legitimate need to be included
- For video conferences, use waiting rooms and passwords where available to enhance security
- Consider whether a conversation is better suited to email or a face-to-face meeting rather than instant messaging

4.4.6 Interaction with Students on Instant Messaging and Video Conferencing

- All communication with students via instant messaging or video conferencing must be for educational purposes only and through school-approved platforms
- Staff must not use personal accounts or platforms to communicate with students
- One-to-one video calls with students should be avoided where possible. If necessary, they must be:
    - Arranged in advance with the student's parent/guardian informed
    - Conducted through the school's approved platforms
    - Recorded or have another staff member present
- Group video calls should have at least two students present, where possible
- Staff should be in an appropriate location for video calls (e.g., not in bedrooms or other private spaces)
- Maintain professional boundaries at all times:
    - Use formal language and tone
    - Avoid sharing personal information or discussing non-school-related topics
    - Be mindful of appropriate dress and background
- Do not initiate or accept friend/contact requests from students on personal instant messaging apps
- Staff must report any concerns about a student's wellbeing or safeguarding issues arising from online interactions immediately to the Designated Safeguarding Lead
- Keep a record of any one-to-one conversations with students, noting the date, time, and brief content
- Be aware that all communications can be monitored and may be subject to disclosure in safeguarding investigations or legal proceedings
- If a student attempts to engage in inappropriate conversation or shares concerning content, end the interaction immediately and report it to the Designated Safeguarding Lead
- Remind students of appropriate online behaviour and the school's expectations for their conduct on these platforms

4.5 Photography and Videography

4.5.1 Consent

- Comply with requirements outlined in the Taking, Storing and Using Images of Children Policy (TSUICP)
- Ensure appropriate consent has been obtained before taking or using photos/videos of students
- TSUICP Multimedia Consent from both parents and students is stored in the iSAMS Pupil Manager module
- The Communications Department will:
    - be aware of all students who have declined consent and must not be photographed or filmed
    - Inform teaching and other departments when new students have declined consent

4.5.2 Storage and Sharing

- Store images and videos of students securely on school systems
- Do not share images of students on personal social media or other non-school platforms

4.5.3 AI-Generated Content, Deepfakes, and Digital Manipulation

The rapid development of Artificial Intelligence (AI) presents both opportunities and challenges. This section outlines the acceptable use of AI-generated content within the Abingdon Foundation environment. For comprehensive guidelines, staff must also refer to the separate Staff AI Guidance document.

“AI-Generated Content” refers to any content (text, images, audio, video, code, etc.) created or significantly modified by artificial intelligence systems. Examples include, but are not limited to:

‘Deepfakes’:

- Realistic but fabricated videos or audio recordings created using AI, often depicting individuals saying or doing things they never did

Synthetic Text:

- Text produced by AI language models (e.g., essays, reports, emails)

Manipulated Audio/Images:

- Audio recordings or images altered or created by AI tools

Acceptable Use Guidelines

The use of AI-generated content within the school environment must adhere strictly to the following guidelines:

- The creation, possession, or sharing of AI-generated content that is illegal, harmful, offensive, obscene, pornographic, discriminatory, constitutes harassment or bullying, or promotes extremism or violence is strictly prohibited
- This includes the creation or distribution of malicious deepfakes depicting any member of the Foundation’s community
- Violation of this rule will result in disciplinary action, up to and including dismissal
- Using AI-generated content to impersonate staff, pupils, or other individuals, or to create and spread misinformation, is strictly forbidden
- Such actions can cause significant harm, reputational damage, and disruption
- All use of AI tools and generated content must align with existing school policies, including the Staff Code of Conduct, Safeguarding Policy, Data Protection Policy, and Social Media Policy

The use of AI tools must comply with the school's Data Protection Policy and the Staff AI Guidance.

- Personal or sensitive data relating to pupils, staff, or other individuals must not be input into public or unauthorised AI tools
- Use authorised school AI tools like Chat Abingdon and Google Gemini, if in doubt, please contact IT

Reporting Misuse

- Staff must report any concerns regarding the misuse of AI-generated content, suspected deepfakes, or breaches of this section immediately
- Safeguarding concerns related to AI-generated content (e.g., deepfakes targeting pupils, cyberbullying using AI) must be reported directly to the Designated Safeguarding Lead
- Other concerns regarding policy breaches or misuse by staff should be reported to the IT Department or the Head, as appropriate
- The school will support affected community members through appropriate channels, including potential counselling and assistance with content removal

4.5.4 Images Taken on Personal Devices

At Abingdon Prep School, no images should be taken on personal devices and staff should refer and adhere to Staff Section of the APS Mobile Technology Policy.

- If images or videos of pupils are taken on a personal device (such as during field trips, sporting events, or other school activities), they must be:
    - Transferred to school equipment or approved secure storage (e.g., Google Drive) as soon as practicable, ideally the same day
    - Immediately and permanently deleted from the personal device after transfer
    - Never stored on personal cloud storage (iCloud, personal Google Photos, Dropbox, etc.)
- Staff must be able to demonstrate compliance with this requirement if requested
- Any exception to this procedure requires explicit prior approval from the Designated Safeguarding Lead

4.6 Filtering and Monitoring

4.6.1 Governance

- In accordance with the Keeping Children Safe in Education (KCSIE) guidance, Abingdon School's governing body is responsible for ensuring that appropriate filtering and monitoring systems are in place to safeguard pupils
- The governing body delegates the day-to-day oversight of these systems to the Designated Safeguarding Lead (and the Senior and Prep Schools) and the IT Director, who work closely together

- The DSL is responsible for ensuring that the filtering and monitoring systems effectively safeguard pupils from potentially harmful and inappropriate online material
- The effectiveness and appropriateness of the filtering and monitoring systems are formally reviewed at least annually at the governor level

4.6.2 Internet Filtering Implementation

The school employs advanced, real-time content filtering technology that inspects all web traffic, including encrypted connections, to effectively identify and block inappropriate content based on actual page content rather than just URLs.

System Scope

- The school employs robust filtering systems to block access to inappropriate content across its networks. Filtering is active 24/7 on school-provided devices, regardless of their physical location. Staff must not attempt to bypass these filters

Mandatory Filtering

- We are committed to filtering access to all criminal websites currently listed on the Internet Watch Foundation's 'Child Sexual Abuse Material' (CSAM) URL list and the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Content Categories (Students)

- For students, filtering targets inappropriate online content, including, but not limited to: Discrimination, Drugs & Substance Abuse, Extremism, Gambling, Hate Speech, Malware / Hacking, Pornography, Piracy and copyright theft, Self-Harm, and Violence

Content Categories (Staff)

- For staff using school networks or devices, filtering targets a subset of categories, including: Extremism, Hate Speech, Malware / Hacking, Pornography, and Violence

BYOD Network Filtering

- The Staff BYOD network utilises the same filtering rules to block inappropriate content categories. While general web browser history on the BYOD network is not routinely decrypted, logged or stored, attempts to access websites blocked by the filter *are* recorded, including user identity, location, device, and the blocked URL
- These blocked access logs are reviewed periodically by the IT Director, and they will report deliberate or repeated attempts to access inappropriate websites

4.6.3 Monitoring Scope, Privacy, and Data Access

While this section details the technical implementation of filtering, the school reserves the right to monitor its IT systems more broadly.

Staff can find detailed privacy and monitoring information in Section 6. Privacy Expectations and System Monitoring.

4.6.4 Self-Disclosure of Potential IT Concerns

- The school recognises that staff may occasionally encounter web blocks or access content that could be misconstrued.
- To promote transparency, a Self-Disclosure of Potential IT Concerns Google Form is available for staff to report such incidents proactively
- Staff are encouraged to use this form promptly after unintentionally triggering a block or viewing potentially inappropriate content
- Timely self-disclosure provides context and can prevent misunderstandings if the activity is flagged during checks
- Information provided is treated confidentially, but does not guarantee immunity if a policy violation occurred, though it will be considered a mitigating factor

4.7 Boarding House IT Management

4.7.1 Extended Duty of Care in Boarding Houses

- Heads of House and boarding staff have an extended duty of care regarding pupils' use of technology in the residential setting
- This includes monitoring and supervising IT use during evenings, weekends, and overnight periods to ensure pupils' wellbeing, adequate sleep, and healthy social development
- Boarding staff must be particularly vigilant regarding potential online safeguarding concerns that may emerge during non-classroom hours

4.7.2 Heads of House's Responsibilities

Heads of House are responsible for implementing and enforcing appropriate house-specific guidelines for technology use that align with this policy while addressing the unique residential context.

These responsibilities include:

- Establishing and enforcing appropriate evening/night-time usage limitations to protect pupils' sleep hygiene
- Monitoring for excessive device use that may impact boarders' social development or academic performance
- Ensuring an appropriate balance between online and offline activities
- Regularly reviewing and assessing the effectiveness of house-specific IT usage guidelines

- Communicating clearly with boarding pupils about expectations for responsible technology use

4.7.3 Boarding House-Specific Network Access

- Boarding houses implement house-specific network access schedules and restrictions as appropriate to the age and needs of their boarders
- Any house-specific restrictions should be clearly communicated to pupils at the beginning of each academic year and when updates occur
- Network access in boarding houses may be limited or suspended during designated hours (e.g., after lights-out) to promote healthy sleep patterns
- The IT Department will support Heads of House in implementing and maintaining appropriate technical controls specific to boarding house networks

4.7.4 Reporting and Managing Concerns in the Boarding Context

- Heads of House should maintain regular communication with the Designated Safeguarding Lead regarding any technology-related concerns identified in the boarding environment
- Heads of House should document recurring patterns of concerning behavior related to technology use
- For minor breaches of acceptable use within the boarding context, Heads of House may implement proportionate disciplinary measures in line with house policies
- Serious or repeated violations should be escalated following the standard reporting procedures outlined in Section 2.4 of this policy

4.7.5 Supporting Healthy Technology Habits

- Boarding staff should actively promote and model healthy technology habits, including appropriate breaks, balanced usage, and technology-free social activities
- Heads of House should provide opportunities for boarders to engage in meaningful offline social interaction and activities, particularly during evenings and weekends
- Educational initiatives within boarding houses should address digital wellbeing topics, including online reputation management, healthy screen time, and sleep hygiene

5. Mobile Devices and Remote Access

5.1 Use of Personal Devices (BYOD)

5.1.1 Permitted Use

- Staff may access school systems and data on personal devices, provided they adhere to this policy
- Personal devices must be equipped with current security software and have encryption enabled
- The Foundation provides a dedicated Staff BYOD Wi-Fi network for convenience, allowing connection of up to three devices simultaneously

- Staff BYOD Wi-Fi credentials are individual and must not be shared
- Basic user activity, location, and timestamp information on the BYOD network are recorded
- The BYOD network employs the same filtering restrictions as the Staff Wi-Fi network
- General web browsing history on the BYOD network is not stored. As detailed in Section 4.6.2, only attempts to access websites blocked by the school's filter are logged and may be investigated
- While not actively monitored, audit records of BYOD network usage are maintained and may be reviewed when necessary
- Use of personal mobile devices during work hours should not interfere with job responsibilities
- Mobile devices should be silenced or on vibrate mode during meetings and lessons

5.1.2 Device Security

Before using any personal device to access school systems (including email, iSAMS, or other school applications), staff must complete the following security checklist:

Personal Device Security Checklist

Staff must answer 'Yes' to ALL of the following questions before using a personal device to access any school system, email, or application:

1. Is your device protected with a strong password, PIN, or biometric authentication (fingerprint/face recognition)?
    - Your device must have active protection to prevent unauthorised access
2. Is your device running the latest available operating system version, or at minimum a version that still receives security updates?
    - Outdated operating systems often contain known security vulnerabilities
3. Is your device free from modification such as jailbreaking (iOS) or rooting (Android)?
    - Modified devices bypass built-in security controls and are vulnerable to attacks
4. Do you only install applications from official sources (Apple App Store, Google Play Store, Microsoft Store)?
    - Third-party app sources often lack security vetting and may contain malware
5. Is automatic updating enabled for your applications, or do you regularly update them manually?
    - Outdated applications may contain security vulnerabilities
6. Do you have device encryption enabled? (This is enabled by default on modern iOS devices and many Android devices)
    - Encryption protects your data if your device is lost or stolen
7. Has your device been kept free from malware? (No suspicious behavior, unexpected pop-ups, or performance issues)
    - Infected devices can compromise school data and credentials
8. If you are using a laptop or desktop computer, do you have active antivirus/security software installed?

    - Security software helps detect and prevent malicious activity

If you answered 'No' to ANY of the above questions, you MUST NOT use that device to access school systems, email, or applications until the issue is resolved. Contact the IT Service Desk for guidance if needed.

Staff members are responsible for maintaining the security of their personal devices. Regularly review this checklist to ensure continued compliance, especially after operating system updates or when changing devices.

5.1.3 Data Protection

- Storage of sensitive school data on personal devices is prohibited unless explicitly authorised in advance by your line manager and is absolutely necessary
- Any school data stored on personal devices must be promptly removed once no longer required
- Staff are responsible for ensuring that their use of personal devices does not compromise school data security

5.1.4 Mobile Network Usage on Personal Devices

- Staff must be aware that using personal mobile data networks (such as 4G, or 5G) on personal devices while on school grounds bypasses the school's network filtering and monitoring systems
- Notwithstanding the network used, all standards outlined in this ICT Acceptable Use Policy apply equally when accessing the internet or online services via personal mobile data networks on school premises
- Users remain accountable for ensuring their online activity via any network connection on school grounds or on school business adheres to the school's professional conduct, safeguarding, and security expectations

5.2 School-Issued Mobile Devices

5.2.1 Acceptable Use

- School-issued mobile devices (including mobile phones and Apple iPad tablets) are primarily for work-related purposes
- Any personal use of these devices must adhere to the conditions outlined in Section 3.2 (Personal Use)
- Staff must not use school-issued devices for any purpose that could bring the school into disrepute

5.2.2 Device Care and Security

- Staff are responsible for the safekeeping and appropriate use of school-issued devices
- Devices must be password-protected and have automatic locking enabled
- Any loss, theft, or damage must be reported immediately to the IT department

- School-issued mobile devices are secured with the same web filtering and monitoring 24/7
- Mobile devices are centrally managed, enabling analysis of usage, software deployment, and device location tracking

5.2.3 Data Management

- Staff should regularly back up important data from mobile devices to school-approved cloud storage, Google Drive
- Confidential or sensitive data should not be stored on mobile devices unless absolutely necessary and encrypted
- Upon termination of employment, all school data must be removed from the device before returning it

5.2.4 Software and Applications

- Staff must not attempt to circumvent the school's mobile device management software
- Only approved applications should be installed on school-issued devices
- Staff should not connect school-issued devices to unknown or unsecured networks

5.2.5 Device Return

- School-issued mobile devices remain the property of the school and must be returned upon request or termination of employment
- Failure to return a device may result in the staff member being charged for its replacement

5.2.6 Monitoring and Privacy

- Staff should be aware that activity on school-issued mobile devices may be monitored
- Personal use of school-issued devices should be limited, and users should not expect privacy for non-work-related activities

5.3 Remote Access

5.3.1 Approved Methods

- Most systems are cloud-based, allowing access to those applications from any location
- Staff must not use public Wi-Fi networks to access internal school systems unless they are using a secure VPN connection
- Access to certain internal school systems remotely requires the use of a school-provided Virtual Private Network (VPN)
- VPN access is granted specifically to staff members whose roles require such access (e.g., Finance) and to staff travelling overseas on official school business

- If you believe your role requires VPN access, or if you are travelling abroad for school purposes, please contact the IT Service Desk for guidance and setup
- School-provided VPNs are not routinely available for general remote working or personal travel

5.3.2 Security Precautions

- Ensure that home Wi-Fi networks are secure and password-protected
- Log out of all school systems when work is completed
- When using public Wi-Fi (such as in hotels, conferences, or coffee shops), be vigilant about spoofed networks. Verify the exact network name with staff of the establishment, as attackers may create similarly-named networks to intercept your data. When in doubt, use your mobile data connection instead or ensure you're using a school-approved VPN

5.4 Remote Working

5.4.1 Data Protection

- When working remotely, take extra care to protect sensitive information
- Avoid printing confidential documents at home

5.4.2 Professional Conduct

- Maintain the same standards of professionalism when working remotely as when on school premises
- Ensure a suitable environment for video calls, considering background and potential interruptions

5.4.3 Overseas Travel

Staff travelling overseas, particularly to countries considered high-risk for cybersecurity, must take extra precautions. This includes ensuring devices are fully updated, using strong passwords/MFA, and enabling encryption.

For travel on official school business

- A school-provided VPN will typically be arranged (see Section 5.3.1).
- Please liaise with the IT Department well in advance

For personal travel

- Staff are strongly advised to use a reputable commercial VPN service when accessing any public or untrusted Wi-Fi networks
- While the school does not provide VPNs for personal travel, the IT Department can offer general advice on selecting commercial VPN services on a case-by-case basis, but staff are responsible for procuring and managing their own service

5.5 Tracking Devices and Technology

The use of personal tracking devices (e.g., GPS trackers, Bluetooth tags like AirTags) on school grounds or during school-related activities requires careful consideration due to potential privacy implications. Staff must adhere to the following guidelines:

- The use of tracking devices by staff is generally permitted only for the purpose of locating personal belongings (e.g., keys, bags)
- The use of tracking devices to monitor the location of individuals (colleagues or pupils) without their explicit knowledge and consent, or appropriate safeguarding justification, is strictly prohibited
- While this policy primarily addresses staff, staff should be aware that parents/guardians may use tracking devices for their children. If a staff member becomes aware that a pupil is being tracked (e.g., via a device in their bag or worn), and has concerns about the appropriateness or potential impact on the pupil or others, they should report this to the Designated Safeguarding Lead
- The school reserves the right to discuss the use of such devices with parents/guardians if concerns arise regarding privacy, distraction, or misuse
- The use of personal tracking devices on school trips should align with the principles outlined above. Any school-sanctioned use of tracking technology for groups (e.g., for safety) would be managed separately and communicated clearly

6. Privacy Expectations and System Monitoring

6.1 Monitoring of IT Systems

6.1.1 Scope of Monitoring

- Abingdon School reserves the right to monitor all aspects of its IT systems and networks
- This includes but is not limited to, Google Workspace, email communications, internet usage, file storage, and network activity

6.1.2 Purpose of Monitoring

Monitoring may be conducted for the following purposes:

- To ensure the security and effective operation of IT systems
- To detect and prevent misuse of school resources
- To investigate potential breaches of school policies or legal requirements
- To comply with legal obligations or lawful requests from authorities

6.1.3 Automated Monitoring

- The school employs automated systems to monitor and filter internet traffic
- These systems may block access to websites deemed inappropriate or a security risk
- The IT Director collates and reports on blocked website alerts every 90 days

- If required, web block reports are sent to the DSL, DFO and the Head

6.2 Privacy Expectations

6.2.1 Limited Expectation of Privacy

- The surveillance services used by IT are strictly controlled, and their usage is audited
- The school does not routinely access staff web activity, emails or other communications
- However, staff should be aware that they should have a limited expectation of privacy when using school IT systems
- This applies to all data stored on or transmitted through school systems, including email, personal files, and full webpage decryption
- Web activity is recorded, stored and may be recalled if needed for legitimate purposes
- Emails and other electronic communications can be used as evidence in disciplinary or court proceedings

6.2.2 Scope of Monitoring

The school reserves the right to monitor, intercept, and review, without prior notification or authorisation from staff:

- Internet usage
- Email and other electronic communications
- File storage and transfers
- Any other use of school IT systems and equipment

6.2.3 Purposes of Monitoring

Monitoring may be conducted for the following purposes:

- To ensure the effective operation of school systems
- To protect against unauthorised access or data breaches
- To investigate suspected breaches of school policies
- To comply with legal obligations or lawful requests from authorities
- To safeguard students and staff

6.2.4 Access to Monitoring Data

- Access to monitoring data is strictly limited to authorised personnel
- Any access to monitoring data will be logged and subject to audit

6.2.5 Personal Use

- While limited personal use of IT systems is permitted, staff should have no expectation of privacy for any activity conducted or data stored on school-owned

computers and systems, as outlined in sections 6.2.1 and 6.2.2. All use of school IT systems should be in accordance with the School's Code of Conduct for staff.

- For personal devices connected to the Staff BYOD Wi-Fi network, privacy expectations differ slightly. The school does not decrypt, inspect, or routinely store the content or history of your web traffic on the BYOD network. However, basic connection data (user, device, time, location) is logged, and attempts to access blocked content will be recorded (see Section 4.6.2)
- Staff should also be aware that if they use some personal accounts on School devices (particularly personal Gmail accounts) or their work accounts on personal devices, that unless they turn 'google sync' off (that will sync basic details across user profiles), it is possible that browser search history performed on non-work devices may be stored on their work devices and therefore become accessible on examination of the device.

6.2.6 Transparency and Notification

- The school is committed to being transparent about its monitoring practices
- Staff will be notified of any changes to monitoring practices unless doing so would compromise a legitimate investigation or legal compliance

6.2.7 Data Protection

- All monitoring activities will be conducted in compliance with the Data Protection Act 2018 and the UK GDPR
- Personal data collected through monitoring will be processed fairly and lawfully, and only retained for as long as necessary
- Emails can be forwarded easily and should not be treated as confidential, any confidential or personal information should be encrypted

6.2.8 Right to Explanation

- Staff have the right to request an explanation of any monitoring or accessing of their data
- Such requests should be made in writing to the Compliance Officer

6.3 Access to User Accounts and Data

6.3.1 Circumstances for Access

The school may access user accounts and data in the following circumstances:

- As part of routine system maintenance
- To investigate safeguarding or disciplinary issues, suspected misuse or policy violations
- To comply with legal obligations or lawful requests
- To ensure business continuity in the absence of a staff member

6.3.2 Authorisation for Access

- Access to user accounts or data must be authorised by the IT Director or a member of the Senior Leadership Team
- Any access will be limited to what is necessary for the specific purpose

6.4 Notification of Monitoring

6.4.1 General Notice

- This policy serves as notice that all use of school IT systems (including wifi use) may be monitored
- Additional reminders may be displayed on school systems or devices

6.4.2 Specific Monitoring

- Where specific, targeted monitoring of an individual's use is deemed necessary, the school will endeavour to inform the individual unless doing so would prejudice legitimate investigations

6.5 Data Retention

6.5.1 Retention of Monitoring Data

- Data collected through monitoring will be retained only for as long as necessary
- Retention periods will comply with legal requirements and the school's Data Retention Policy