ST PAUL'S CATHEDRAL SCHOOL

Acceptable Use of ICT Policy (Staff)

Academic Year 2025-2026

Review Date: March 2026

Aims and Principles

St Paul's Cathedral School is a Christian, co-educational community which holds to the values of love, justice, tolerance, respect, honesty, service and trust in its life and practice, to promote positive relationships throughout the school community and where the safety, welfare and emotional well-being of each child is of the utmost importance.

The school aims to instil a love of learning through a broad curriculum. It aims to give each pupil the opportunity to develop intellectually, socially, personally, physically, culturally and spiritually. All pupils are encouraged to work to the best of their ability and to achieve standards of excellence in all of their endeavours.

Through the corporate life of the school, and through good pastoral care, the school encourages the independence of the individual as well as mutual responsibility. It aims to make its pupils aware of the wider community, espouses the democratic process and encourages a close working relationship with parents and guardians.

Contents:

Statement of intent

St Paul's Cathedral School believes that ICT plays an important part in both teaching and learning over a range of subjects, and the school accepts that both school-owned and personal electronic devices are widely used by members of staff. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.
The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff are responsible users and remain safe while using the internet.
- School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the Online Safety Policy.

1. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Education (Independent school Standards) Regulations 2014
- EYFS statutory framework for group and school-based providers (DfE, November 2024)
- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Staff Code of Conduct
- Safeguarding Policy and Child Protection Policy Procedures
- Online Safety Policy
- Complaints Policy

2. Roles and Responsibilities

The Trustees with the Board of Governors has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The Head is responsible for:

- Reviewing and amending this policy with the Deputy Head, Head of ICT, the Compliance Manager, and the IT Manager, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources. This duty is delegated to the Director of Finance and Operations, Head of IT and IT Manager.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.

The IT manager is responsible for:

- Monitoring internet activity of all user accounts and to report any inappropriate use to the headteacher and or DSL
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the headteacher.

- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.
- Ensuring routine security checks are carried out on all school-owned devices and personal mobile phones that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Ensuring that, though appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- Disabling user accounts of staff who do not follow this policy, at the request of the headteacher.
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of personal devices to the Bursar who is the Data Protection Officer.

The Director of Finance and Operations as the Data Protection Officer is responsible for:

- Ensuring that all school-owned and personal electronic devices have security software installed, to protect sensitive data in cases of loss or theft.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

Staff members are responsible for:

- Requesting permission from the headteacher or IT Manager, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours and ensuring these devices are submitted for security checks on an annual basis.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the DPO.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the headteacher.
- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

The Director of Finance and Operations is responsible for:

- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made.
- Overseeing purchase requests for electronic devices.

- **Classifications**

School-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards
- Mouse
- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Fax equipment
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

3. Acceptable Use

This policy applies to any computer or other device connected to the school's network and computers.

The school will monitor the use of all ICT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.

Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.
Any member of staff found to have breached the school's Data Protection Policy or relevant legislation may face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the headteacher.

School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.
Members of staff ~~will~~ should not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files (over **500MB**) without permission from the ICT technician.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.

All data will be stored appropriately in accordance with the school's Data Protection Policy.

Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.

School-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings are applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.
School-owned devices will be taken home for work purposes only, once approval has been sought from the headteacher. Remote access to the school network will be given to staff using these devices at home.

School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the headteacher.
While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a school-owned phone for personal use will be permitted for necessary calls.

Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the headteacher.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

4. Emails and the Internet

The school email system and internet connection are available for communication and use on matters directly concerned with school business.

Unprofessional or abusive messages will not be tolerated. All emails should be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications

All emails being sent to external recipients will contain the school standard confidentiality notice. That notice will normally be configured as a signature by the IT Manager and will not be removed.

Personal email accounts will only be accessed via school computers outside of work hours and only if they have built-in anti-virus protection approved by the IT Manager. Staff will ensure that access to personal emails never interferes with work duties.

Staff may link work email accounts to personal devices, subject to the IT manager's approval. Staff are required to have device encryption and are prohibited from downloading and storing personal data, eg. Pupils' details.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for school equipment will only be permitted to be made online with the permission of the headteacher, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the Financial Controller. This is in addition to any purchasing arrangement followed according to the school's Finance arrangements.

Any suspicious emails will be recorded by the IT manager and will be reported to the headteacher. All incidents will be responded to in accordance with the Online Safety Policy.

Portable Equipment

All data on the school network is backed up on a daily basis.

Portable school-owned electronic devices should be kept out of sight and stored securely when they are not in use.

Portable equipment should be transported in its protective case, if supplied.

Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.

5. Personal Devices

Staff members will use personal devices in line with the school's Code of Conduct and Online Safety Policy.

All personal devices that are used to access the school's online portal, systems or email accounts, e.g. laptops or mobile phones, are required to have device encryption and regular software updates. Mobile phone should be submitted for routine checks.

Multi-Factor Authentication is required for e-mail access on devices, including personal devices used for school purposes outside of the school premises. E-mail access off-site will not be permitted without MFA.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.

Members of staff will not contact pupils or parents using their personal devices.

Inappropriate messages will not be sent to any member of the school community.

Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken. Wherever possible staff should use equipment provided or authorised by the School; if a personal device is authorised to be used, the pictures must be immediately uploaded (within one working day) to school systems and deleted from the personal device; cloud storage systems should be disabled

Specific guidelines for the use of cameras, mobile phone and electronic devices are in place for staff working with EYFS children (Appendix 1).

Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be stored securely.

6. Removable Media

Only recommended removable media will be used including, but not limited to, the following:

- DVDs
- CDs
- USB drives

Personal and confidential information will not be stored on any removable media.

Personal USB drives should not be used without permission from the IT Manager.

7. Cloud-based Storage

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

8. Unauthorised Use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the headteacher.
- Physically damage ICT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the IT Manager or headteacher. Certain items are asset registered and security marked; their location is recorded by the Director of Finance and Operations for accountability. Once items are moved after authorisation, staff will be responsible for notifying the Director of Finance and Operations of the new location.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. Users will change their passwords when requested by the IT Manager of SLT. User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
- Any material that is illegal
- Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
- Online gambling
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
- Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the IT Manager or the headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.
- Use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Purchase any ICT facilities without the consent of the Line Manager, IT Manager or headteacher.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the headteacher. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.

- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the Finance Policy.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the headteacher. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher.
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the headteacher.

9. Safety and Security

The school's network will be secured using firewalls in line with the Data Protection and Online Safety Policy.

Filtering of websites, will ensure that access to websites with known malware are blocked immediately and reported to the IT Manager.

Approved anti-virus software and malware protection will be used on all approved devices and is constantly auto updating.

The school will use mail security technology to detect and block any malware transmitted via email – this will be reviewed on an annual basis.

Members of staff will ensure that all school-owned electronic devices are made available for anti-virus updates, malware protection updates and software installations, patches or upgrades, when required.

Staff are expected to take suitable precautions to ensure personal devices used for school purposes remain secure at all times.

Programmes and software will not be installed on school-owned electronic devices without permission from the IT Manager.

Staff will not be permitted to remove any software from a school-owned electronic device without permission from the IT Manager.

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the IT Manager, may be subject to disciplinary measures.

All devices will be secured by a password or biometric access control.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time. This will be no more than 10 minutes for mobile or other portable devices and 15 minutes for desktop computers or laptops.

All devices must be encrypted using a method approved by the IT Manager.

10. Monitoring and Review

This policy will be reviewed annually by the Deputy Head, Head of IT and the IT Manager.

Appendix One: EYFS POLICY FOR THE USE OF CAMERAS, MOBILE PHONES AND ELECTRONIC DEVICES

To ensure the safety and welfare of the children in our care this policy outlines the protocols for the use of personal mobile phones and cameras in the setting. This policy will be used across the whole of the Pre-prep department.

• Personal mobile phones, cameras and video recorders (and all other electronic devices with imaging and sharing capabilities) cannot be used when in the presence of children either on school premises or when on outings.

• All mobile phones must be locked and stored securely within the setting. (This includes all staff, visitors, parents, volunteers and students).

• No parent is permitted to use their mobile phone or use its camera facility whilst inside school buildings. School policy regarding this matter should be explained clearly to Parents by the Head of Pre-prep or Head of Early Years.

• Mobile phones must not be used in any teaching area within the setting.

• In the case of a personal emergency staff should use the school telephone. It is the responsibility of all staff to make families aware of the school telephone numbers.

• Personal calls may be made in non-contact time but not within the teaching areas.

• Personal mobiles, cameras or video recorders should not be used to record classroom activities. ONLY school equipment should be used.

• Photographs and recordings can only be transferred to and stored on a school computer before printing.

• All telephone contact with Parents/Carers must be made on the school telephone and should be recorded.

• During group outings nominated staff will have access to the school mobile which can be used in an emergency or for contact purposes.

• In the case of school productions, Parents/carers are permitted to take photographs of their own child in accordance with school protocols which strongly advise against the publication of any such photographs on social networking sites.

Monitoring and Review: It is the responsibility of all staff to adhere to this policy. It will be reviewed annually by the Governing body.

Spring Term 2025 MSS, Head of Pre-prep

Appendix Two: Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.
By signing this form, you are declaring that you have read, understood and agree to the terms of the Staff Acceptable Use of Technology Policy. You should read and sign the declaration below before returning it to the **school office**.
Members of staff are required to re-sign this declaration form if changes are made to the policy.

I have read the school's Staff Acceptable Use of Technology Policy and understand that:

- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the headteacher.
- Illegal, inappropriate or unacceptable use of school or personal equipment will result in disciplinary action.
- The school reserves the right to monitor my work emails, phone calls, internet activity and document production.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

Name of staff	
Job title	
Department	
Signed	
DSL signed	
Headteacher signed	
Date signed	