Saint Pierre School,

16 Leigh Road, Leigh-on-Sea, Essex SS9 1LE

ICT Acceptable Use and Digital Safety Policy

Policy Owner (Position)	Last Updated By (Name)	Date of Last Review	Date Next Review Due	
Headmaster	Peter Lane	8th Oct 2024	8th Oct 2025	
Read in Conjunction with: **ICT Online Filtering and Monitoring Policy** Online Safety Policy ICT Pupil Acceptable Use ICT Acceptable Use E-Safety Policy Staff code of conduct				

Contents

1 Introduction 1

2 Purpose of this Policy 2

3 Scope 2

4 Related Documentation 3

5 Roles and Responsibilities 3

6 Safe Use of Technology 3

7 The Right to Use School Network and Equipment. 4

8 Appropriate Use of Technology for Digital Safety 5

9 School Allocated Devices: Access & Privacy 8

10 Photographs and Images 8

11 Artificial Intelligence 9

12 Use of School equipment for personal use 10

13 Use of personal equipment in School 10

14 Procedures for Reporting 10

15 Removal of Network Rights/Sanctions 11

1 Introduction

1.1. The use of technology as a tool has become an integral part of school and home life.

1.2. Saint Pierre School is committed to the effective and purposeful use of technology for teaching, learning and administration and is also committed to protecting its staff, students, parents and visitors, from illegal or harmful use of technology by individuals or groups, either knowingly or unknowingly.
1.3. The school actively promotes the participation of parents to help the school safeguard the welfare of pupils and promote the safe use of technology.
1.4. This policy applies to the use of:

- All technology devices and equipment connected to the school network;
- All technology devices supplied by the school to employees and contractors, both onsite and offsite;
- All applications and IT services provided by the school for teaching, learning and administration; and
- All applications and IT services available online and accessible via the school network or a school technology device.

1.5. A copy of this policy is available to staff, students, parents and visitors on request and on the school website.
1.6. In the event of a breach of this policy and its requirements, failure to have read this policy will not be accepted as a defence/excuse.

2 Purpose of this Policy

2.1 Promote responsible use and care of technology and IT services available to staff, students, parents and visitors;
2.2 Outline the acceptable and unacceptable use of technology and IT services at the school, both on and offsite;
2.3 Outline the roles and responsibilities of all staff, students, parents and visitors;
2.4 Educate and encourage pupils to make good use of the educational opportunities presented by access to technology at the school
2.5 Safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

- exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);
- inappropriate contact from staff;
- inappropriate contact from strangers;
- cyber-bullying and abuse;
- copying and sharing personal data and images;
- etc.

2.6 Outline Digital Filtering and Monitoring on school devices and the school network.
2.7 Outline requirements for reporting misuse of technology.

3 Scope

3.1 This policy applies to all staff, students, parents and visitors of the school.

3.2 The school will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing

and communications devices, network hardware and software and services and applications associated with them including:

- the school network, WIFI and internet access;
- tablets, desktops, laptops, and thin client devices;
- mobile phones, smartphones, smart watches and other smart wearables;
- digital devices for audio, still images and moving images (e.g. personal music players and GoPro devices);
- digital displays and SMART boards;
- 2D and 3D printers;
- communication and collaborations applications (e.g. email and Teams);
- Virtual Learning Environments (e.g. firefly);
- mobile messaging apps (e.g. Snapchat and WhatsApp); and
- social media (e.g. Facebook, Instagram, TikTok);
- etc.

3.3 This policy applies to the use of technology on and off school premises.

3.4 This policy applies to any member of the school community where the culture or reputation of the school are put at risk.

3.5 This policy applies to any member of the school community where staff, students, parents or visitors are put at risk.

4 Related Documentation

4.1 Safeguarding and Child Protection Policy
4.2 Preventing Radicalisation and Extremism Policy
4.3 Promoting Good Behaviour Policy

5 Roles and Responsibilities

5.1 This policy document is the responsibility of the Head/ Proprietor

5.2 The school Head is responsible for publishing this policy and the ongoing implementation and monitoring of this policy.

5.3 All staff, students, parents and visitors are responsible for adhering to the policy.

6 Safe Use of Technology

6.1 The school is committed to the safe and purposeful use of technology for teaching, learning and administration.

6.2 Use of technology should be safe, responsible, respectful to others and legal. Staff, students, parents and visitors are responsible for their actions, conduct and behaviour when using technology at all times.

6.3 The school will support the use of technology and make internet access as unrestricted as necessary whilst balancing the educational needs of our students, the safety and welfare of staff, students, parents and visitors, and the security and integrity of our systems.

6.4 Monitoring, logging and alerting tools are in place to maintain technology safety, safeguarding and security for the protection of Staff, Students, Parents and Visitors.

6.5 In the interest of safeguarding children, student 1-to-1 devices have monitoring software preinstalled. The software provides live and historic data regarding the use of the device e.g. web browsing, and the data collected is stored for 90-day periods.

6.6 We want pupils to enjoy using technology and to become skilled users as technology has become a fundamental part of education, not only as the vehicle to deliver great teaching and learning, but as a platform for collaboration and productivity.

6.7 Pupils will be educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

6.8 The school actively encourages the participation of parents to help promote the safe use of technology with their children.

6.9 Any concern regarding unsafe or inappropriate use of technology should be reported to a teacher, school Head or Designated Safeguarding Lead as soon as possible.

6.10 Any serious incident involving unsafe or inappropriate use of technology will be reported by the school Head who may decide to involve the Police.

6.11 All users of technology may find the following resources helpful in keeping themselves safe online:

- UK Safer Internet Centre
- Internet Matters - resources
- Google Family Safety
- Common Sense Media

7 The Right to Use School Network and Equipment.

7.1 School employees will be allocated a username and password for accessing technology devices and services.

7.2 Some shared resources will have a generic username and password for access.

7.3 All school technology remains the property of the school. The school may reasonably request the device or withdraw access to the service at any time and, if applicable, the device must be returned to the school.

7.4 Only school devices should be connected to the school network without written permission from the Headmaster

7.5 Any attempt to access or use any user account or email address, for which a staff member, student, parent or visitor is not authorised, is prohibited.

7.6 Designated devices may be issued to school employees and students for teaching, learning and administration:

- Students with a designated device may use the device in lessons at the direction of their teacher.
- School employees and students are responsible for the safety and security of a designated device when taken out of school.
- School issued devices and associated peripherals should be returned in good condition (excluding ordinary wear and tear) and in
- Staff / Parents are responsible for the cost of a like for like replacement of an assigned device if it is damaged / lost intentionally, wilfully or through neglect.

7.7 School employees and students may not use, or attempt to use, IT resources allocated to another person, except when explicitly authorised.

7.8 For security purposes users must log off or lock their computer at all times when they step away from their device. Users must log-off and shutdown their device at the end of the day.

8 Appropriate Use of Technology for Digital Safety

8.1 The school provides System and Application Accounts for staff, students, parents and guests when required.

Staff and students must:

- o Not allow other people to use your account.
- o Not use someone else's account. o Lock your device or logout of your account when not in use.
- o Only use school applications and email for official school business and digital correspondence.
- o Not send messages or emails from school accounts that purport to come from an individual other than the person actually sending the message.
- o Use official school accounts on approved collaborative platforms

8.2 The school provides technology Hardware and Software to support education and the running of the school business.

- Users of school technology equipment are expected to take care of the equipment through responsible behaviour.
- School technology should not be removed from school site except where:
    - The device is assigned to an individual member of staff; or
    - The device is assigned to a student via the 1-to-1 programme; or
    - There is written permission from a member of the School Leadership Team.
- School technology assigned to staff and students is the responsibility of the assignee.
- You should not leave portable technology equipment, including school-issued devices unattended.
- Loss or damage of school technology should be reported to a teacher or member of the School Leadership Team
- Theft of school technology assigned to an individual member of staff or to a student via the 1-to-1 programme should be reported to the police and be reported to a teacher, member of the School Leadership Team at the earliest opportunity along with a crime reference.
- Deliberate abuse or damage of school equipment will result in the culprit(s) being billed for the full replacement costs of the equipment.
- Do not:
    - Attempt to install software onto a school-owned or school-issued device other than when directed to by the Headmaster.
    - Download or access illegal software on school devices.
    - Download any software packages from the school network onto portable media or personal devices.
    - Attempt to copy or remove software from a school-owned or school-issued device.
    - Attempt to alter the configuration of the hardware equipment or any accompanying software unless under the written instruction of the school.

8.3 The school provides technology resources for accessing and storing Data.

- Do not:
    - Access or attempt to access data for which you are not authorised.
    - Interfere with digital work belonging to other users.
    - Share private, sensitive or confidential information unless:
        - You have authority to share
        - The method of sharing is secure
- It is the responsibility of technology users when accessing data to be aware of Intellectual property rights infringement including copyright, trademark, patent, design and moral rights.

8.4 The school endeavours to safeguard and where possible mitigate all Security risks associated with technology.

- The school has filtering systems in place to block access to unsuitable material, wherever possible and to protect the welfare and safety of staff, students, parents and guests.
- You must not:
    - o Try to bypass school filtering systems whilst using school devices or using the school network.
    - o Use software or network routing designed to bypass filters and access blocked sites.
    - o Try to bypass technology security systems whilst using school devices or using the school network.
    - o Use software or network routing designed to bypass school technology security systems.
- Access to unsuitable material on a school device or on the school network should be reported to a teacher, member of the School Leadership Team at the earliest opportunity.
- The school has technology security systems in place to block and to protect against computer viruses or other malicious software such as spyware.
- Concerns regarding viruses and other malicious software should be reported to a teacher, member of the School Leadership Team at the earliest opportunity.

8.5 It is the responsibility of all technology users to ensure the Welfare of themselves and others both on personal and school devices.

- Cyberbullying - Pupils must not use their own or the school's technology to bully others.
- Strangers - Pupils must not use their own or the school's technology to make contact or engage with people who they do not know.
- Sexting - Pupils must not use their own or the school's technology to create or share sexualised content including images, audio, video and text.
- Concerns regarding welfare associated with use of technology should be reported to a teacher, or member of the School Leadership Team or Designated Safeguarding Lead at the earliest opportunity.

8.6 The school provides appropriate access to the Internet and Social Media to support education and the running of the school business.

- The internet provides technology users with unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisation and groups world-wide so as to increase skills, knowledge and abilities.
- The school actively supports access to the widest variety of information resources available, accompanied by the development of the skills necessary to filter, analyse, interpret and evaluate information encountered.
- Staff, students, parents and visitors must not use a school device or the school network to intentionally visit internet sites that contain obscene, illegal, hateful, abusive, offensive, pornographic, extremist or otherwise inappropriate materials.

- Staff, students, parents and visitors must not use a school device or the school network to access gambling websites.
- Staff, students, parents and visitors shall be responsible for notifying a member of the School Leadership Team, or Designated Safeguarding Lead of any inappropriate material accessed on a school device or on the school network so that access can be blocked.
- Privacy of staff, students, parents and visitors must always be recognised and respected on social media sites.
- Staff should not connect with any pupil under the age of nineteen on any social networking site or via personal mobile phones.
- Staff, students, parents and visitors of the school must not make offensive or inappropriate comments including bringing the school's name and reputation into disrepute on any forum/platform, such as social media sites where a connection between the user and the school can reasonably be made.

9 School Allocated Devices: Access & Privacy

9.1 Access to assigned devices and IT content:

- School technology devices assigned to staff and students are for the sole use of the assignee.
- School devices may be loaded with Remote Support Applications which enables IT support staff to logon to the devices to provide remote assistance; this may only be used with the permission of the device assignee.
- The school reserves the right to access an assigned device and monitor it's use and content under the following special circumstances including but not limited to:
    - o To detect and/or prevent crime.
    - o To enable system security protection (e.g. Virus, Malware, Hacking or other Risk).
    - o To investigate potential misuse, abuse and/or illegal activity.
    - o To monitor compliance with employment and statutory obligations.
    - o To guarantee the integrity of the school devices, technology and IT systems.

10 Photographs and Images

10.1 The school abides by data protection legislation, namely, the General Data Protection Regulation 2018 (as amended, extended or re-enacted from time to time), and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as a yearbook or on a parent portal. Parents and guardians may withdraw this permission at any time by informing the school's SLT Team in writing.

10.2 The School does not permit the use of personal mobile phones and cameras by staff where children are present, see mobile device policy

10.3 The Early Years Safeguarding and Welfare Requirements requires all schools to have a clear policy on the use of mobile phones and devices.
10.4 Staff, students, parents and visitors are not permitted to use devices such as mobile phones, cameras, smart watches or digital recorders to photograph or record members of staff or pupils without their permission. Safe and appropriate use of recording equipment must be discussed with the pupils as part of the curriculum and referred to whenever recording is to take place. Permission may be granted by the school in the event of performances/events organised by the school.

10.5 Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission. Any parent who does not wish for their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

11 Artificial Intelligence

11.1 Staff Use Of AI

- All usage must be transparent and honest – staff must not pass off AI-generated work as their own but acknowledge to colleagues and pupils alike the extent of AI assistance.
- AI tools must not be used to impersonate individuals or organisations, in a misleading or malicious manner, or to generate content that is unlawful, harmful, or offensive.
- Use of AI tools and data/content created using such tools must comply with the following policies: Staff Code of Conduct and the Acceptable Use Agreement.
- AI must not be used to help generate official school pupil or parent-facing correspondence without clearance and checking from an appropriate member of SLT.
- AI must not be used to write or to help write any parts of reports that go to pupils or parents.
- AI must not be used to mark or help assess work without approval from SLT.
- Staff must not give an AI model any personal or professional information about themselves, the school, other staff members, pupils or their families.
- No information about school events or trips using specific locations, or information that makes the school or any individual identifiable, for example to help write risk assessments, may be put into a search engine or AI tool.
- Staff should familiarise themselves with the guidelines about AI use and the potential of AI tools, especially if planning use within a lesson.
- Staff have a responsibility to ensure, if AI is used, sensible and appropriate use, and to

If in doubt about whether use of AI is advisable or allowable, please consult a member of SLT.

11.2 Pupil Use Of AI

- AI tools used in academic work must not be used for cheating, plagiarism, or any other unethical behaviour.

- AI tools must not be used to impersonate individuals or organisations, in a misleading or malicious manner, or to generate content that is unlawful, harmful, or offensive.
- Use of AI tools and data/content created using such tools must comply with the following policies: ICT Pupil Acceptable Use and Behaviour Policy.
- AI-generated content should not be considered a substitute for pupil effort or original work.
- Students are required to put in their own effort to understand the material and produce unique content.
- Students must always clearly credit/acknowledge the use of known AI technology in their work when they have actively engaged with it.
- Students must not disclose any confidential or personal information about themselves or any other people to the AI model since then the information may be in the public domain and accessible to others.

When staff allow the use of AI during lessons they will ensure that all other aspects of the Online Safety policy are also being adhered to.

12 Use of School equipment for personal use

12.1 School devices and IT systems are provided for schoolwork only; should you decide to use the equipment or IT systems for personal use, please be informed that it will be at your sole risk and could be considered as a breach of the Digital Safety Policy. Furthermore, please be informed that as per Section 9 of this Policy, The School is entitled to access and monitor the use and content of the School equipment and technology, including the personal communications that may have been made through those school means.

12.2 Only approved software and applications may be installed on a school device.

12.3 School devices and network must not be used to carrying out any illegal trading activity.

12.4 Conducting any private or financial transaction on shared equipment carries a risk and your personal data may not be safe.

13 Use of personal equipment in School

13.1 Personal devices must not be connected to the school without permission from the Headmaster

14 Procedures for Reporting

14.1 Staff, students, parents and visitors of the school with a concern or an incident regarding technology should take the following actions:
- Stop the problem or remove the technology.
- Prevent exposure of the incident to others.

- Record the nature of the incident and those involved.
- Preserve evidence to enable investigation if required.
- Report the incident or concern to a teacher, school Head, or Designated Safeguarding Lead as appropriate.
- Staff must not carry out any investigations unless they are authorised to do so

14.2 Any concern regarding unsafe or inappropriate use of technology, or welfare associated with use of technology, should be reported to a teacher, school Head or Designated Safeguarding Lead as soon as possible.

14.3 Access to unsuitable material and concerns regarding viruses and other malicious software on a school device or on the school network should be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity.

14.4 Loss, damage or theft of school technology should be reported to a teacher, member of the School Leadership Team at the earliest opportunity; theft should also be reported to the police and a crime reference obtained.

14.5 Pupils must take responsibility for their use of IT equipment both at school and at home; should parents or guardians have concerns or become aware of an issue, we strongly encourage prompt communication with the school so we can offer advice and support.

14.6 The school has a duty to report serious concerns to Local Authority Safeguarding Teams or to the Police, in line with statutory requirements.

15 Removal of Network Rights/Sanctions

15.1 Anyone found abusing the Digital Safety Policy on the use of computers may have their network rights removed and may be subject to further disciplinary action.

15.2 The school reserves the right to remove network access at any time.

15.3 The school may inform the police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

15.4 The school takes its responsibilities in relation to digital safety and use of technology by staff, students, parents and visitors seriously and understands the importance of monitoring, evaluating and reviewing its policies and procedures regularly.