



Saint Pierre School,

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

Online Safety - Policy

Policy Owner (Position)	Last Updated By (Name)	Date of Last Review	Date Next Review Due
Headteacher	Peter Lane	2 Dec 24	2n Dec 25
Read in Conjunction with: ICT Pupil Acceptable Use ICT Acceptable Use and Digital Safety Policy ICT Online Filtering and Monitoring Policy Mobile and Smart Technology Policy Anti-Bullying Policy Safeguarding Policy Mobile Phone Policy Prevent Policy			

Saint Pierre School E- Safety Policy

(COVID change: pupils use of computers may be suspended at the discretion of the headmaster)

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's Online safety policy will operate in conjunction with other policies including those for Safeguarding and Child Protection, Mental Health and Emotional Wellbeing, Promoting Positive Behaviour, Anti-Bullying, Curriculum and our ICT Acceptable Use.

Good Habits

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online safety policy in both administration and curriculum, including secure school network design and use.
- In school, safe and secure broadband including the effective management of content filtering.
- When using WI-FI it should be via a password protected network.
- National Education Network standards and specifications to be adopted at all times.

School Online safety Policy

Our Online safety policy has been written by the school. It has been agreed by the Senior Leadership Team and has been approved by the Proprietor.

The Online safety policy will be reviewed annually.

Why Is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality access Internet access.

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How Does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient in support of remote learning.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between students world-wide.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DfE.
- Communication and progress reporting to parents and carers.

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students (HCC).
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research including, the skills of knowledge location, retrieval and evaluation.

The 4 C's of Online Safety

The school recognises the "4 C's of Online Safety" as published in KCSIE; CONDUCT, CONTENT, CONTACT, COMMERCIALISM

- **Conduct: children may be at risk because of their own behaviour, for example, by sharing too much information:**

Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers. Discuss with your child the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.

- **Content: age-inappropriate or unreliable content can be available to children**

Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias. Children may need your help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

- **Contact: children can be contacted by bullies or people who groom or seek to abuse them**

It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access. If you have concerns that your child is, or has been, the subject of inappropriate sexual contact or approach by another person, it's vital that you report it to the police via the Child Exploitation and Online Protection Centre (www.ceop.police.uk). If your child is the victim of cyberbullying, this can also be reported online and offline. Reinforce with your child the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

- **Commercialism: young people can be unaware of hidden costs and advertising in apps, games and websites**

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Encourage your children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.

Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted Internet access.
- All staff must read and sign the 'ICT Acceptable Use' policy before using any school ICT resources.

- Parents are informed that students will be provided with supervised Internet access.
- Students must agree to comply with 'ICT Pupil Acceptable Use' policy.

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time and content must be reported to the Headteacher.
- Saint Pierre School will make all reasonable efforts to ensure that the use of Internet derived materials by students and staff complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email/MS Teams

- Students may only use the provided school MS Teams account for school-based communications such as sending work home.
- Where online platforms require an email address, students must use the one provided by the school.
- Students must immediately tell a teacher if they receive an offensive message.
- Students must not reveal personal details of themselves to others in an e-mail or MS Teams communication, or arrange to meet anyone without specific permission.

Social Networking

- The school blocks/filters access to social networking sites and newsgroups, unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students should be advised not to place personal photos on any social network space. Students should be advised on security and encouraged to set secure passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Filtering

The school will ensure filtering systems are as effective as possible.

Managing Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Personal mobile devices, such as phones, tablets, smart watches, fitness trackers etc. will not be used during lessons or formal school time unless with SLT permission.
- The sending of abusive or inappropriate communications such as; messages, e-mail, images and videos are forbidden.

Published Content and The School Website

- The contact details on the website will be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Students' Images and Work

- Images that include students will be selected carefully and will be appropriate for the context.
- Permission from parents and carers will be obtained upon admission before any images of students are published on the Internet, in printed publications or on display boards.
- Students' full names will not be used alongside their image anywhere online or in publicity without specific parental permission.

Information System Security

- School ICT systems capacity and security will be regularly reviewed.
- Virus protection will be installed and updated regularly.
- Security strategies will be regularly reviewed.

Protecting Personal and Sensitive Data

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate.

Handling Online safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with School Child Protection procedures.
- Students and parents will be informed of the complaints procedure.

Communication of Policy

Students

- Rules for IT access will be posted in all classrooms.
- Students will be informed that IT use will be monitored and sanctions imposed for misuse.
- Social Media Age Restrictions are shared at least annually with both students and parents via assemblies and e-mail, and with students in IT lessons.

Staff

- All staff will have access to the school Online safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents and Carers

- Parents' attention will be drawn to the school Online safety policy in newsletters, the school prospectus and on the school website.
- Social Media Age Restrictions are shared at least annually with both students and parents via assemblies and e-mail, and with students in IT lessons.
- Parents and carers will be informed of the safeguarding rules for the use of video conferencing for Parents' Evening.
- Safeguarding and online advice will be published for parents.