E-safety Policy

Including internet acceptable use provisions

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Committee responsible:	Full Governing Body
Staff responsible:	Lenia Greenaway
Date approved:	Summer 2025
Review period:	Annual
Next review date:	Summer 2026

This policy has been written by St Peter's School, building on best practice and government guidance. It is in line with Surrey County Council policy for E-safety. E-safety falls within the 'Staying safe' strand of 'Every Child Matters' agenda which we at St Peter's firmly believe in, so that all children will be safeguarded. E-safety is part of the school's safeguarding responsibility. This policy relates to other policies and guidance documents including those for Behaviour management, Child Protection and Safeguarding, Anti-bullying, Data handling and the use of images.

References to 'internet' in this document also includes social media platforms, E-gaming, messaging services and phone/tablet apps

This policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, chrome books, mobile phones, tablets and hand-held games consoles used on the school site.

The E-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff or pupil.

Principles of internet use
Children need every possible opportunity to explore and use new technologies. This will prepare them for the future and their continued learning. Use of the internet is an essential part of education and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet access is an entitlement for pupils and internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Benefits of using the internet in education
Benefits of using the internet in education include:

Benefits for pupils

- To enrich and extend learning activities, making learning engaging and fun.
- To enable pupils to work remotely from home if required due to illness, self-isolating or a local or national lockdown due to exceptional circumstances, for example, Covid-19.
- Access to world-wide educational resources across the curriculum.
- Inclusion in government initiatives, for example Eco Schools and the Olympic website.
- Educational and cultural exchanges between pupils.
- Broaden and embed the development of IT skills used in everyday life.

Benefits for School staff

- To enhance teaching and engage all learners.
- For professional development through access to national developments, educational materials and good curriculum practice.
- To facilitate communication with support services, professional associations and colleagues.
- To improve access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the different education agencies such as Local Authority (LA), Diocese and Department for Education (DfE).

Internet access

- Safe use of the internet (E safety) is part of both the statutory Computing and P.S.H.E./R.S.E. curriculum at St Peter's School.
- Simple rules are agreed with the children (such as 'Think then Click') and displayed in classrooms.
- Pupils will only access the internet when staff are present.
- All class computers and children's chrome books have stringent school filters in line with the measures outlined within KCSIE. Reports of misuse are immediately flagged to the Headteacher.
- Staff will take all reasonable precautions to ensure that users access only appropriate material but it is impossible to guarantee that unsuitable material will never appear on a school computer.
- Internet access will be planned. Suitable internet sites are researched as part of planning and to ensure they are relevant to the age of our children.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for their age and maturity.
- Pupils will be educated in the effective use of the internet for research.
- The school internet access is designed for pupil use and will include filtering appropriate to the age of pupils.
- Access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved, on-line materials.
- Pupils will not be allowed access to chat rooms.
- Pupils will not be issued individual email accounts. Older pupils will be authorised to use a group/class email address under supervision, as appropriate.
- All parents will be asked to sign and return an Internet and E-Safety Agreement form upon their child[ren]'s entry to St Peter's. For EYFS children this is also on behalf of their child to agree to the school's e-safety rules. Pupils in KS1 will sign an ICT agreement to agree the school's e-safety rules termly and EYFS pupils will sign these from the spring term.

Evaluating Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the School Business Manager or Headteacher.
- The School should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Use of email or messaging apps/platforms

- When email/messaging platforms are used as part of learning, the class teacher should always control its use.
- Email/messages sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff may use a school email address to communicate planning etc. but non-school use should be used in exceptional circumstances only. All staff are issued with a school email address.
- Pupils and staff may only use approved e-mail accounts on the school IT system.
- Staff to pupil email communication as per the curriculum must only take place via a school email address.
- Incoming e-mail should be treated with caution and great care should be exercised before opening attachments unless the author is known.

How School website content will be managed

- The point of contact on the website should be the school address, school email and telephone number. Staff or pupils' home information will not be published

- Website photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Filtering

- The school will work in partnership with parents, the LA, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved and are in accordance with the new published standards for 'Filtering and monitoring'.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Headteacher or School Business Manager.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation iwf.org.uk

Staff use of the Internet

- The school internet policy will only be effective if all staff subscribe to its values and methods. Abuse of the internet is a serious matter that could result in disciplinary procedures. Refer to the document Guidance for 'Safer Working Practice for Adults who work with Children and Young People in Education' (Updated Jan 2021) available in the staffroom.
- All staff must accept the terms of the 'School Acceptable Use Policy' as per the Appendix below, before using any Internet resource or mobile technology in school. This also applies to governors and volunteers if they are working with children on computers or other mobile technology.
- All staff including teachers, supply staff, teaching assistants and support staff, will be provided with a copy of this E-safety Policy and its importance will be explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.
- Staff development in safe and responsible internet use and on the school internet policy will be provided as required.
- All staff are expected to adhere to the school's Data Protection Policy at all times

Parents' support

- On entry to the school parents will be informed about the school's E-Safety Policy and where to find it.
- Parents will be asked to sign an 'Internet and E-safety' Agreement as per the Appendix below.
- Internet issues will be handled sensitively to inform parents without causing undue alarm.
- A partnership approach with parents will be encouraged. An ICT/E-safety information session and open morning is held annually and this includes demonstrations of how e safety is taught, practical sessions and advice regarding safe internet/mobile technology use at home. Additional information is given as appropriate.
- While it is recognised that mobile phones are an important part of modern life, parents will be asked not to use mobile phones in school for making and answering calls, sending and receiving messages.

- Parent helping on educational trips must not use their mobile phones during the course of the day for making and receiving calls, sending messages or emails, accessing social media sites or taking photographs; unless in exceptional circumstances and agreed with the headteacher first. It is the responsibility of the teaching staff leader to ensure parents are aware of this policy and the information is communicated to parent helpers.

Use of personal devices

- Personal equipment may only be used by staff to access the school IT systems if their use complies with the school's Data Protection Policy and this E-safety policy.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held accountable for the loss or damage of any personal devices used in school or for school business.
- The Bluetooth functionality of a mobile phone should be switched off at all times and may not be used to send images or files to other mobile phones.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.
St Peter's School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
St Peter's School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

How will complaints about Internet use/E-safety be handled?

- Any complaint about staff misuse must be referred immediately to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with the school child protection and safeguarding procedures.
- Please refer to the response procedures flowchart in Appendix 1 if you have an e-safety concern.

Monitoring

- The application of this policy is monitored by the Headteacher.
- An E-safety audit will be carried out to assess its e-safety provision and identify any gaps by the above named persons.

Other policies relating to E-safety include:

Anti-bullying policy
Child Protection and Safeguarding policy
Data Protection Policy
PSHE – working document
Remote learning policy
RSE policy
Staff disciplinary procedures

For additional information:
Safer Surrey - Surrey Safeguarding Children Partnership
https://surreyscp.org.uk/
'Filtering and Monitoring'
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges

Please refer to the school website for a comprehensive list of E-safety website addresses and systems for reporting on-line abuse or E-safety matters.

** PARENT TO SIGN AND RETURN TO SCHOOL **

Internet and E-safety Parental Agreement

All pupils use computer facilities, including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that E-safety rules have been understood.

Pupil name: .....

Parent / Carer name: .....

- As the parent or legal guardian of the above pupil, I have read and understood the attached E-safety rules and give permission for my child to access the internet, learning platform and other ICT facilities at school.

- I know that my child will be taught the schools E-safety rules and that a copy of these rules is displayed in each classroom. I will ensure my child follows these rules and will support the safe and responsible use of ICT at St Peters School.

- I understand that the school will take all reasonable precautions to ensure that pupils are safe and will not be able to access inappropriate materials. Using an educationally filtered service and with adult supervision this will minimise the risk at school and home.

- I understand that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet.

- I understand that the school can check my child's computer files, Learning Platform activities and websites they visit and that if they have any concerns about their e-safety they will contact me.

- I am aware that long periods of 'screen time' are not advised and that regular breaks should be encouraged.

- I will support the school by promoting safe use of the internet and digital technology at home.

Parent / Carer signature:..... Date:.....

(Further information on E-safety can be found in our E-Safety Policy
under the 'Policies' section of our school website www.stpetersinfant.org)

Internet and E-safety Pupil Agreement

All pupils use computer facilities, including internet access as an essential part of learning, as required by the National Curriculum and Early Years Foundation Stage. Both pupils and their parents/carers are asked to sign agreements to show that E-safety rules have been understood.

Pupil name: .....

- I have understood the school E-safety rules 'Think then Click'.
  My teacher has explained them to me.

- I understand that I must keep my name and passwords a secret when online (I can tell my teachers or parents).

- I understand these rules are to help keep me, my friends, and my family safe.
  I agree to follow these rules.

- I will use the schools computers / chromebooks / Ipads, internet, digital cameras, recorders and other ICT equipment in a safe way.

- I understand that if I do not follow these rules, I may not be allowed to use the internet, or any of the school computers, devices and ICT equipment.

Pupil signature……..

Date…….

School Acceptable Use Policy for ICT
Staff, Governors and Visitors

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are fully aware of their professional responsibilities when using any form of ICT. All staff will sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher. (Please also see Safer Working Practice for Staff in the staffroom.)

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email and social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email, internet, network, Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head Teacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will only use the approved, secure email system (Microsoft Outlook 365) for any school business.
- I will ensure that all electronic communications with parents and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head Teacher or Governing Body. (Refer to Data Security Policy)
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent, carer or staff member. I understand that images will not be distributed outside the school network/learning platform without the permission of the parent/carer, member of staff or Head Teacher.
- These images must only be taken using a dedicated digital camera. This is in order to protect both the pupil and staff member. Mobile phones must not be used for school photographic purposes.

- Any images I take or record on a personal digital camera will be uploaded onto the school system and deleted from the device as soon as possible with a witness present to see the deletion.
- I will respect copyright and intellectual property rights.
- Mobile phones will not be used in any school area other than the staffroom and will be either switched off or turned onto silent mode during school working hours.
- Staff will not use names for children or members of staff when using email, text or social networking sites and will adhere to the privacy setting when using these different social media.
- I will not install any hardware or software.
- I will report any incidents of concern regarding children's safety to the ICT Leader and the Designated Safeguarding Lead/Head Teacher, or DDSL (in their absence).
- I will support the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

User Signature

I agree to follow this code of conduct, the Policy for ICT and the E-Safety Policy and to support the safe use of ICT throughout the school.

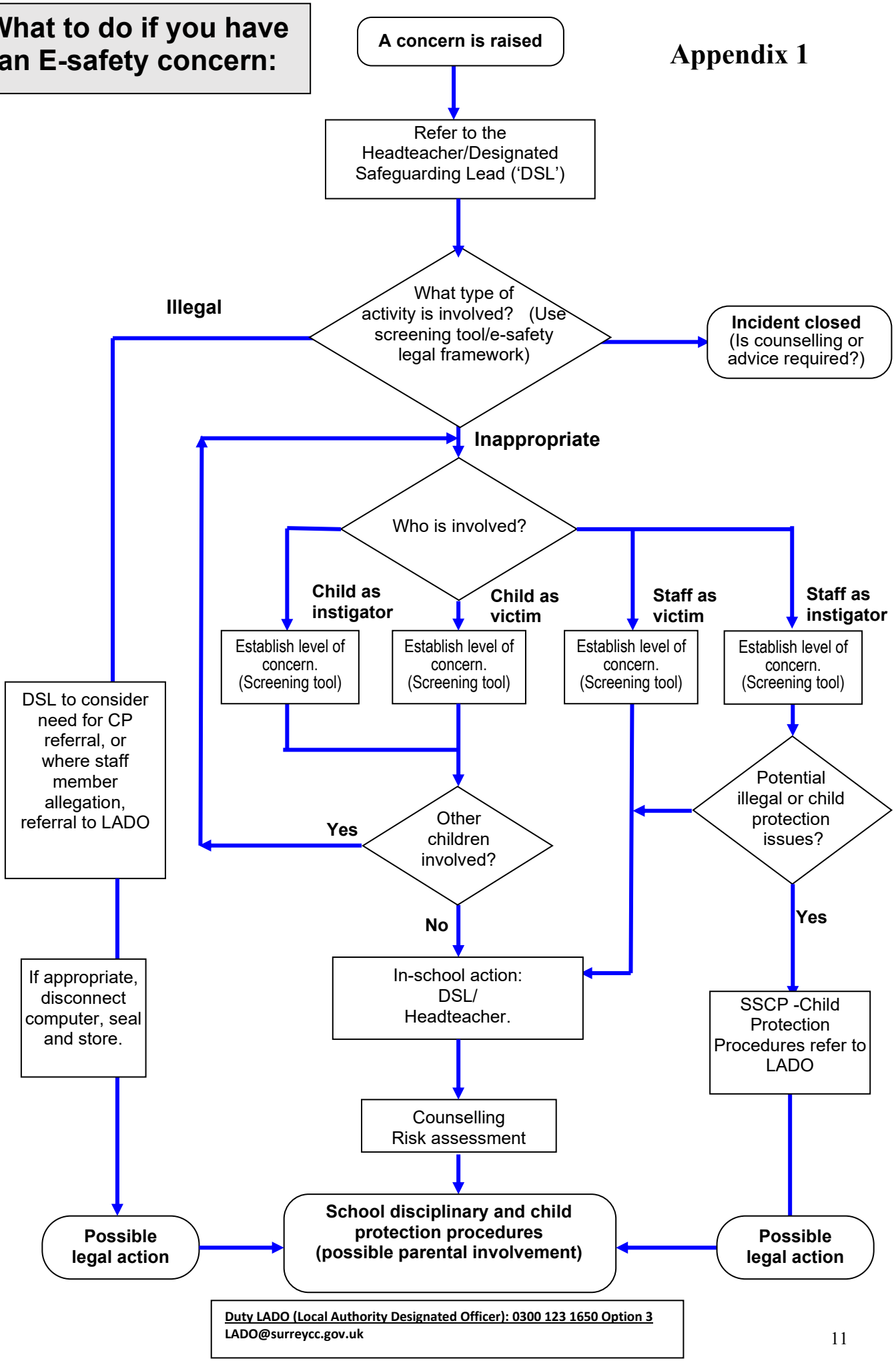
Full Name:.....(printed)

Job Title:.....

Signature:..... Date:.....

What to do if you have an E-safety concern:

Appendix 1



Duty LADO (Local Authority Designated Officer): 0300 123 1650 Option 3
LADO@surreycc.gov.uk