St. Paul's First School E-safety policy

Writing and reviewing the E-safety policy

The E-safety Policy is part of the School Improvement Action Plan and relates to other policies including those for computing, bullying and for safeguarding (child protection).

- The school's E-safety coordinator is Claire Richards, although every member of staff has a responsibility for ensuring children are kept safe and would need to act if an e-safety issue arose.
- We receive professional advice and support from our contracted IT provider, Entrust .
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors; the learning and teaching committee will have responsibility for monitoring that procedures are followed.
- The E-safety Policy and its implementation will be reviewed annually, or more regularly if the need arises.
- School will monitor the impact of the policy using:
  - Logs of reported incidents
  - Monitoring logs of internet activity
  - Surveys of children, carers and staff

Teaching and Learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by Entrust Broadband and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- Pupils will be taught how to evaluate Internet content
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content by informing an adult as soon as possible so that the matter can be dealt with straight away.
- It will be made clear to children that if they have similar issues off site, they can still report this in school. In addition, children will also be encouraged to inform a parent or carer.
- Children will also be told that if they experience any form of cyber-bullying, they should also report this to a member of teaching staff.

Managing Internet Access

Access Information system security

- All pupils and staff have log on details for computer access. If a member of staff leaves or a pupil contravenes our e-safety policy, then access will be withdrawn.
- School IT systems security will be reviewed regularly by Entrust.
- Virus protection will be updated regularly.

E-mail

- Staff may only use approved e-mail accounts on the school system.
- Pupils will not be given school email accounts.

Published content and the school web site

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

Publishing pupils' images and work

- Written permission from parents or carers will be obtained before images of pupils are published on the school website and other social media used by the school.
- Photographs that include pupils will be selected carefully and will not be published without parents' permission. Permissions notifications will be held in the office.
- Pupils' full names will be avoided on the website or other on-line space, including in blogs, forums or wikis, particularly in association with photographs.

- Personal cameras or other electronic devices belonging to children or staff - will not be used to capture images of pupils, other than those staff members who have been authorised by the head teacher.
- The school policy will be on the website, so that parents/carers can have access to information on image taking and publishing, both on school and independent electronic devices.
- Children will not be permitted to take any electronic devices with internet connectivity or camera facility on residential trips. This will be communicated to parents as and when trips take place.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must not place personal photos on any social network space provided at school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school will work in partnership with Staffordshire County Council and Entrust to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and the adult concerned will assess the suitability for its use in school in discussion with the e-safety co-ordinator and/or the Headteacher.
- Ipad cameras may be used as part of a lesson. The use of Ipads will be closely monitored by staff to ensure inappropriate use does not occur.
- Staff will use the school phone where contact with parents of pupils is required, or will endeavour to block their number if a personal phone needs to be used in extraordinary circumstances. This can be done by typing 141 before the required number.
- Mobile phones and associated cameras will not be used during lessons. The sending of abusive or inappropriate text messages is forbidden.
- Children's mobile phones are not permitted in school.

- A school mobile will be used for trips.
- Pupils will only use video conferencing devices for an educational activity when this has been agreed by a teaching member of staff.
- Staff must not use personal mobile devices to send/receive calls or texts whilst they are responsible for children (eg during lessons or clubs). Mobile phones must be handed into the school office on entering the school. Staff should provide school contact details for family and others to use in the event of an emergency. This applies to all volunteers and students as well.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will be able to access school data remotely from the server, but must not use this facility in a public place and ensure that they log off when leaving their computer unattended. They must be mindful of who may have access to an unsupervised laptop.
- Encrypted flash drives will be provided when necessary.
- Members of staff are responsible for ensuring the security of flash drives in their possession.
- All issued flash drives need to be returned when a member of staff leaves.

Policy Decisions

Authorising Internet access

- The school will allow all staff access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site. Assessing risks
- The school will take all reasonable precautions to prevent access to inappropriate material, through the school's filtering systems. 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. Neither the school nor Staffordshire LA can accept liability for the material accessed, or any consequences of Internet access.
- The school computing and E-Safety coordinators will audit IT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the head teacher.

- Complaints of a child protection nature must be dealt with in accordance with school safeguarding (child protection) procedures.
- Pupils and parents will be informed of the complaints procedure, if a complaint arises.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy. This will be published in the School Lettings Policy.

Communications Policy

Introducing the E-safety policy to pupils

- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils. There are very close links between our E-safety policy and PSHE policy and curriculum, as well as the school behaviour policy and code of conduct. All children are provided with an E-safety assembly each year on SID (Safer Internet Day) to advertise and teach about different aspects of E-safety, delivered by the E-safety coordinator.

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained.
- All staff are expected to sign the school's Acceptable Use Policy (AUP) as part of annual refresher training on E-safety, provided by the E-safety coordinator and Child Protection Lead (CPL).
- 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.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School E-safety Policy in the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety as part of school run E-safety workshops, led by the school's E-safety coordinator and CPL.

- The school will ask all new parents to sign the parent/pupil agreement when they register their child.

Approved by staff: October 2017
Agreed by governing body: October 2017
To be reviewed: Autumn 2018