

William Penn e-Safety Policy

William Penn Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that e-Safety encompasses not only internet technologies, but also electronic communications such as mobile phones and wireless technology.

This policy should be read in conjunction with the Safeguarding and Child Protection Policy.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones and personal digital assistants (PDAs);
- Internet communications: e-mail and IM;
- Webcams and videoconferencing;
- Wireless games consoles.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This e-Safety Policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

People acting inappropriately or even illegally cause these risks to e-safety. Any potential issue is dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents vary from the prank or unconsidered action, to considered illegal activity.

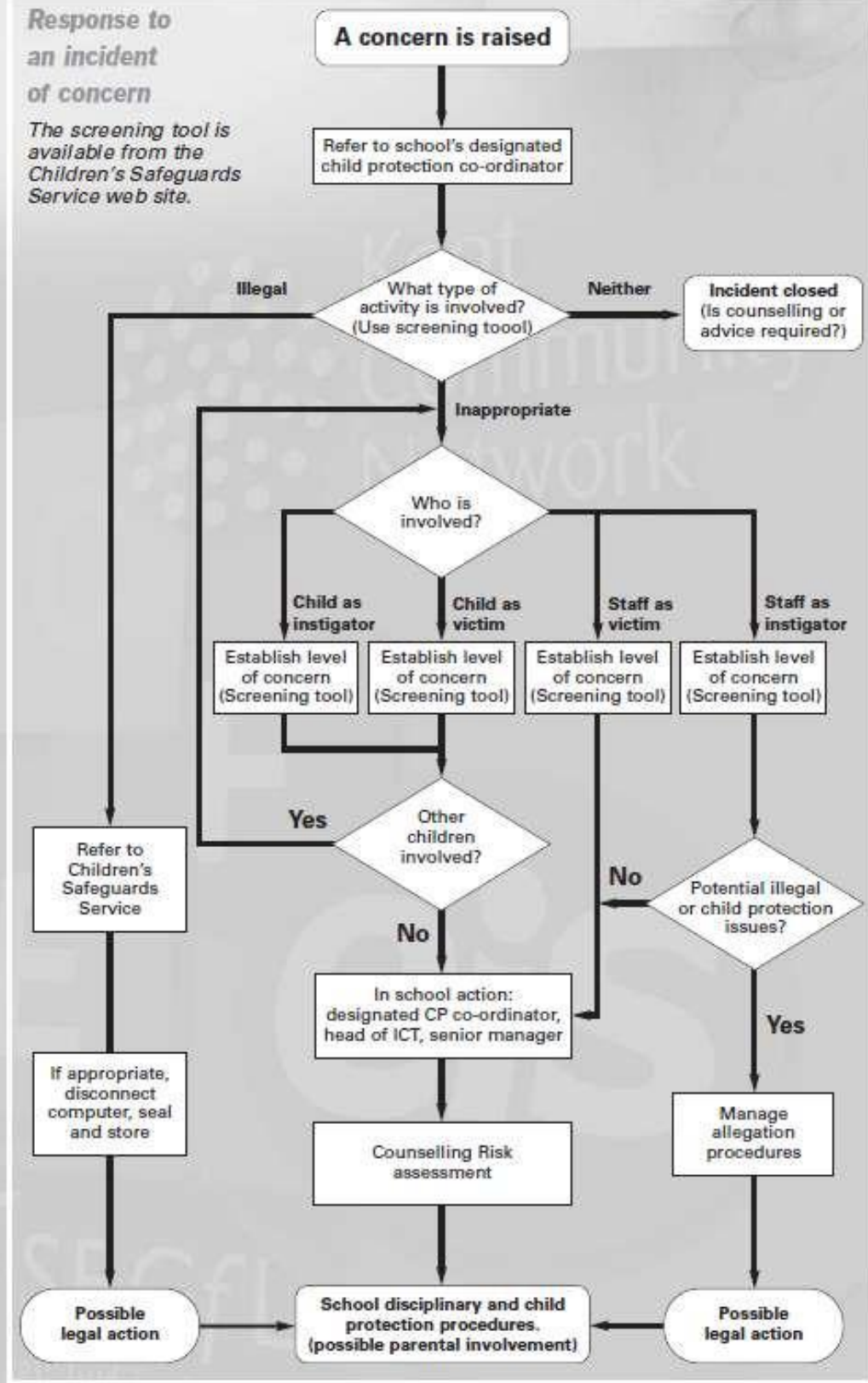
What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

The flowchart on the next page illustrates our approach to investigating an incident of concern. This diagram should not be used in isolation when responding to incidents.

Response to an incident of concern

The screening tool is available from the Children's Safeguards Service web site.



A summary of a school's e- safety responsibilities is outlined below. This list will assist in developing a co-ordinated and effective approach to managing e-safety issues.

- The school e-Safety Coordinator may also be a Designated Safeguarding Lead as the roles overlap, but could also be a member of SMT, the ICT Coordinator or a subject teacher. The e-safety Coordinator may seek support and advice from the county e-Safety Officer, and where necessary, the Police. At William Penn the e-safety lead is also the computing lead.
- The e-Safety coordinator maintains the e-Safety Policy, manages e-Safety training and keeps abreast of local and national e-safety awareness campaigns. The school reviews the policy regularly and revises the policy annually to ensure that it is current and takes in to consideration, any emerging technologies.
- The school reviews the filtering systems regularly to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse are investigated.
- The school includes e-Safety in the curriculum and ensures that every pupil has been educated about safe and responsible use. Pupils know how to control and minimise online risks and how to report a problem.
- All staff and pupils read and sign the Acceptable Use Policy (parents may sign on behalf of young children having discussed e-safety with them).
- The e-Safety Policy is made available to all staff, governors, parents and visitors through the website.

Implementation and Compliance

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational IT experiences.

Teaching and learning

Why is Internet use important?

Developing effective practice in internet use for teaching and learning is essential.

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 functions. The internet use is part of the statutory curriculum and a necessary tool for learning. 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. Pupils use the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

Pupils are taught what internet use is acceptable, and what is not, and given clear objectives for internet use.

- Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils;
- Staff guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity;
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating Internet Content

In a perfect world, inappropriate material would not be visible to pupils using the internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school ensures that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

Local Area Network Security

- Users act reasonably;
- Users take responsibility for their network use. For all staff, flouting acceptable use policy is regarded as a matter for dismissal;
- Workstations are secured against user mistakes and deliberate actions, e.g. deleting files and folders;
- Servers are located securely and physical access restricted;
- The server operating system is secured and kept up to date;
- Virus protection for the whole network is installed and current;
- Access by wireless devices is pro-actively managed.

Wide Area Network (WAN) security

All internet connections are arranged via Exa to ensure compliance with the security policy. Firewalls and switches are configured to prevent unauthorised access between schools.

- The security of the school information systems is reviewed regularly;
- Virus protection is updated regularly;
- Security strategies are discussed with the LA when necessary;
- Personal data sent over the internet is encrypted or otherwise secured;
- Portable media is not used without specific permission followed by a virus check;
- Unapproved system utilities and executable files are allowed in pupils' work areas or attached to e-mail;
- Files held on the school's network are regularly checked;
- The ICT co-ordinator / network manager reviews system capacity regularly.

Emails

- Pupils do not use email accounts in school.

School Website and Learning Platform

The contact details on the website comprise of the school address, e-mail and telephone number. Staff or pupils' personal information is not published. E-mail addresses are published carefully, to avoid spam harvesting. The Head Teacher takes overall editorial responsibility and ensure that content is accurate and appropriate. The website complies with the school's guidelines for publications including respect for intellectual property rights and copyright.

Use of Images

Images that include pupils are selected carefully and comply with the school's media permission terms.

Social Networking – please refer to Social Media Policy and Use of Mobile Phones and Digital Photography Policy

- The school blocks/filters access to social networking sites;
- Newsgroups are blocked unless a specific use is approved;
- Children are taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations:

Pupils are advised, never to give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc

- Pupils are advised not to place personal photos on any social network space;
- They consider how public the information is and consider using private areas;
- Advice is given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school;
- Teachers do not to run social network spaces for students to use on a personal basis.

Filtering

The school works with the IT systems administrator and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL is reported to the e-safety Coordinator.

This task requires both educational and technical experience. Senior staff ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Google Classroom Accounts

All pupils and staff are issued with unique user names and passwords. Google Classroom is used in school and at home. Email and Google Hangout have been disabled on the students' accounts.

Video Conferencing

Google Meets is used when remote learning takes place and in school when required. Parents have been issued with a Parent Guide and Expectations document that clearly states how children should behave in order to keep themselves safe during these video meetings.

Emerging Technologies

Emerging technologies are examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones are to be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 but with due regard given to the principles of GDPR May 2018.

Internet Risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor West Sussex County Council can accept liability for the material accessed, or any consequences resulting from internet use.

The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

E Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff;
- All children will be taught to use the internet safely and the role of CEOP to monitor and report abuse;
- Any complaint about staff misuse must be referred to the Head Teacher, unless it is the Headteacher where complaints will be sent to the Chair of Governors;
- Pupils and parents will be informed of the complaints procedure;
- Parents and pupils will need to work in partnership with staff to resolve issues.

Introducing the Policy

- Safety rules will be posted in rooms with internet access;
- Pupils will be informed that network and internet use will be monitored;
- Safety training will be introduced to all to raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede internet access;
- An e-safety module will be included in the RSE, Citizenship or IT programmes covering both school and home use;
- All staff will be given the school e-Safety Policy and its application and 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 IT use will be supervised by senior management and have clear procedures for reporting issues;
- Parents' attention will be drawn to the school's e-Safety Policy in newsletters and on the school website;
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- Staff attention will be drawn to the increased vulnerability of pupils with SEN to risk online; especially those with language and communication difficulties. Usage by these pupils must be closely monitored.

Websites offering additional advice and guidance:

Childline

<http://www.childline.org.uk/>

Child Exploitation & Online Protection Centre

<http://www.ceop.police.uk/>

<https://www.thinkuknow.co.uk/>

Internet Watch Foundation

<http://www.iwf.org.uk/>

Childnet

<https://www.childnet.com/>

Action for Children

<http://www.actionforchildren.org.uk/what-we-do/about-us/our-history/>

NSPCC

<https://www.nspcc.org.uk/>

Virtual Global Taskforce – Report Abuse

<http://virtualglobaltaskforce.com/>

Signed:

Date approved: 30.3.22

Date of Next Review: Summer 2023