Penygaer Primary School

Online Safety Policy

September 2026

Penygaer Primary School Online Safety and Acceptable Use Policy

Introduction

- The Online Safety Policy relates to other policies including those for ICT and Child Protection.
- The school's Online Safety Coordinator is the ICT Coordinator, currently the deputy headteacher.

Why Internet Use Is Important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

Internet use will enhance Learning

- The school Internet access is designed expressly for pupil and staff use 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 to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will raise awareness of issues of copyright regarding the use of Internet derived materials by staff and pupils.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

E-mail

- Pupils may only use approved e-mail accounts on Office 365 within HWB
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communications, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mails from pupils to external bodies is presented and controlled.

Published content and the school web site

• Staff or pupil personal contact information will not generally be published. The contact details given online is the the school office.

• The deputy headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

• Generally pupils' names will not be used in association with photographs anywhere on the school Web site or other on-line space such as social media etc.

• Pictures and work will only be shown on the website if parents/carers have given consent issued at on entry to the school.

• Parents will be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

• The school will control access to moderated social networking sites in HWB and j2Launch and consider how to educate pupils in their safe use.

• Pupils will be advised never to disclose personal passwords.

• Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

• Pupils will be advised never to upload pictures/videos of themselves or their friends to any Internet site.

• 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.

• Where personal cameras are used in school or on trips, awareness of appropriate use will be fully discussed with all pupils.

• Risk assessments prior to school visits will take account of any children going on a visit who do not have parental permission for photographs to be taken.

• Permission will be sought from parents to use pupils' photos on social media, the school website and YouTube.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.
- Some older pupils who walk/cycle to school may bring mobile phones but must be handed in immediately to the class teacher for safe keeping until the end of school. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Children will be made aware of responsible use of these machines.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Procedures

- The school ICT system's security will be reviewed regularly.
- Virus protection is updated regularly through the Local Authority's filter system.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Coordinator who will alert the Local authority. The Online Safety Coordinator will be informed.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequence of Internet access.
- The school will regularly audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective. It will continue with the 360°safe self-review tool.
- The audit will be carried out by the ICT Co-ordinator annually and findings recorded.
- Online Safety training is embedded within the ICT scheme of work and the Health and Well-being areas of learning.
- Online Safety briefings and materials will regularly be made available to parents.
- Staff will always use a suitable and safe search engine when accessing the web with pupils.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a

member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first, and appropriate professional language should always be used.

Handling Online Safety complaints

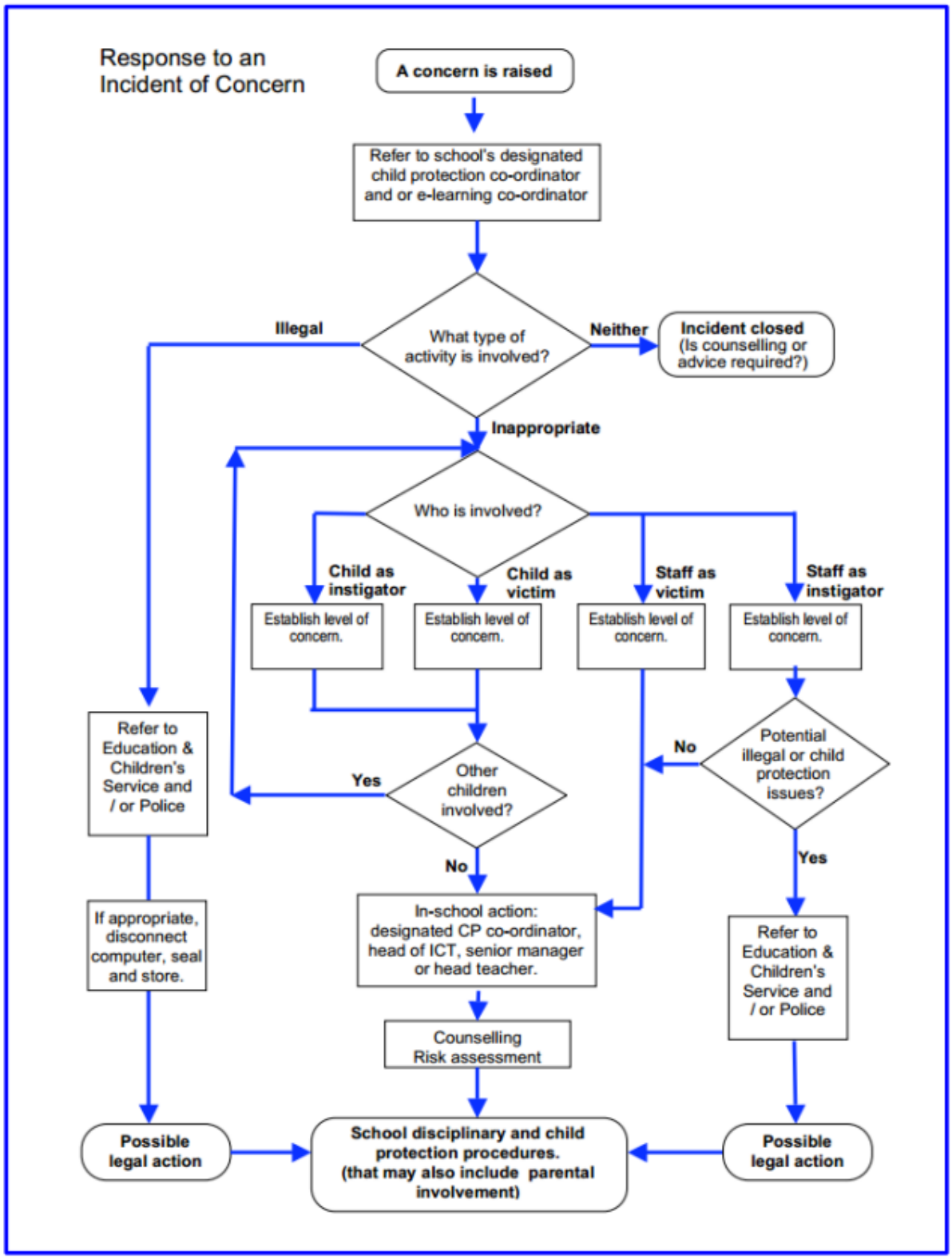
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (See Child Protection Policy)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- The following flowchart will give a clear path of action for all staff, should an online safety incident occur.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school Web site.
- The school will ask all parents to sign the parent agreement regarding the use of photographs when their child starts school. This is a permission form when they start at the school.

For further advice please contact the school.

Signed: Mrs Helen Conway (Headteacher)	
Signed: Mr Richard Samuel (Chair of Governors)	


Response to an Incident of Concern
A concern is raised
Refer to school's designated child protection co-ordinator and or e-learning co-ordinator
What type of activity is involved?
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern.
Establish level of concern.
Establish level of concern.
Establish level of concern.
Refer to Education & Children's Service and / or Police
Other children involved?
Yes
No
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager or head teacher.
Refer to Education & Children's Service and / or Police
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (that may also include parental involvement)
Possible legal action

Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property, and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Online Safety Coordinator or the Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct for Penygaer Primary School.

Signed .....

Initials .....

Date / /