Pensans CP School

On Line Safety Policy

Written: September 2018
Review Date: September 2019

Pensans Primary School
On-line Safety Policy 2018

Pensans School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Pensans we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

On-line safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Pensans School.

Our On-Line Safety Policy has been written following government guidance. It has been agreed by senior management and approved by governors.

The school's On-Line Safety coordinator is Angela Clay, the On-Line Safety Governor is Graham Mills. The On-Line Safety Policy and its implementation shall be reviewed annually.
It will be reviewed in the Autumn term 2019 as part of our safeguarding review

Roles and Responsibilities
Governors:
Governors are responsible for the approval of the On-Line Safety Policy and for reviewing the effectiveness of the policy. The role of the On-Line Safety Governor will include:

- Regular meetings with the On-Line Safety Committee.
- Regular monitoring of On-Line Safety incident logs.
- Reporting to the Behaviour & Safety Committee.

Headteacher and Senior Leadership Team:
The Headteacher is responsible for ensuring the safety (including on-line safety) of members of the school community, though the day-to-day responsibility for on-line safety will be delegated to the On-line Safety Coordinator.
The Headteacher/Senior Leaders are responsible for ensuring that the On-Line Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their On-Line Safety roles and to train other colleagues, as relevant.
The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal On-Line Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
The Headteacher and Assistant Head should be aware of the procedures to be followed in the event of a serious On-Line Safety allegation being made against a member of staff.

The On-Line Safety Coordinator:
- Takes day-to day-responsibility for On-Line Safety issues and has a leading role in establishing and reviewing the school On-Line Safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an On-Line Safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of On-Line Safety incidents and creates a log of incidents to inform future On-Line Safety developments.

All School Staff

All staff, including non-classroom based staff, will receive regular training and updates regarding on line safety, cyber-bulling, sexting, Child Exploitation and Radicalisation, including face to face and online training sessions as appropriate to ensure that they are aware of the latest developments. They will all be aware of the flow chart of procedures to follow in the case of an online safety incident.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

The school Internet access will be designed expressly for pupil use, including appropriate content filtering. Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

As part of the 2014 Computing curriculum, all year groups have digital literacy units within the iCompute Scheme of Work that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.

Children also receive a discreet series of lessons in the Autumn term to address On-Line Safety, including cyber-bulling, sexting, Child Exploitation and Radicalisation delivered in a way that is appropriate to each year group. The school currently uses the ‘Know-it All’ and ‘Think You Know’ Scheme of Work.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion,language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi- ethnic society. We also measure and assess the impact regularly through meetings our SEN co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Authorised Internet Access

By explicitly authorising use of the school’s Internet access pupils, staff, governors and parents are provided with information relating to On-Line Safety and agree to its use:

All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource. Parents will be informed that pupils will be provided with supervised Internet

access and asked to sign and return a consent form for pupil access.
Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:
If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an On-Line Safety Log, which will be stored in the Classroom. Staff will follow the procedures detailed in the Appendix with regard to reporting incidences of a serious nature. The On-Line Safety Logs will be reviewed monthly by the On-Line Safety Co- ordinator. The school will work in partnership with NCI, the provider of the school's filtering system to ensure that these are as effective as possible at all times. This will be reviewed annually.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of On-Line Safety:
Pupils may only use approved e-mail accounts on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
Whole class or group e-mail addresses should be used in school rather than individual addresses.

Access in school to external personal e-mail accounts is not allowed.
E-mail sent to external organisations should be written carefully and authorised by the teacher in charge before sending.
All official communications which are work related must be sent by staff to and from their work email address as supplied by the school.
Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' their laptop if they are going to leave it unattended.

Social Networking

Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the On-Line Safety policy need to be recorded ivy the headteacher and the governor for On-line Safety. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Child Protection Officers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Phase Leader in the same day.

Allegations involving staff should be reported to the Headteachers. If the allegation is one of abuse then it should be handled according to the DFE document titled ‘Dealing with allegations of abuse against teachers and other staff’. If necessary the local authority’s LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the class teacher at 8:50 and collected at the end of the day.
The sending of abusive or inappropriate text messages is forbidden.

Staff should always use the school phone to contact parents.
Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.

Staff may use their mobile phones in the staffroom/one of the school offices.
Parents cannot use mobile phones on school trips to take pictures of the children

On trips staff mobiles are used for emergency only.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.
Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.

Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

One of the Headteachers or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera or iPad to capture images and should not use their personal devices. The exception to this is where a camera has been logged by the On-Line Safety Coordinator and the serial number of the camera noted.
Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.
Contact details on the Website will be the school address, e-mail and telephone number.
Staff and pupils' personal information will not be published.
The Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographs and videos that include pupils will be selected carefully and will not include children for whom permission to use their photo has not been granted.
Pupils' full names will not be used in association with photographs.
Consent from parents will be obtained before photographs of pupils are published on the school Website.

Work will only be published with the permission of the pupil.

Parents should only upload pictures of their own child/children onto social networking sites.
The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

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

Security strategies will be discussed and reviewed regularly by the Online Safety Committee and our filtering suppliers and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

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

Assessing Risk

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 does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the On-Line Safety policy is adequate and that the implementation of the On-Line Safety policy is appropriate.

Handling On-Line 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 one of the Headteachers. Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
Pupils and parents will be informed of the complaints procedure.
Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:
Rules for keeping safe on-line will be posted in all rooms with ICT equipment.
Pupils will be informed that Internet use will be monitored.
Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

All staff will be given the School On-Line Safety Policy and its importance explained.

Parents:

Parents' attention will be drawn to the School On-Line Safety Policy in newsletters and on the school Website.

Appendices:

- Student / Pupil Acceptable Usage Policy
- Staff and Volunteers Acceptable Usage Policy
- Parents / Carers Acceptable Usage Policy Agreement
- School Filtering Policy
- School Password Security Policy
- School Personal Data Policy
- School E-Safety Charter
- Ideas for schools to consider
- Legislation
- Links to other organisations and documents
- Resources
- Glossary of terms