Pupil Premium Awards 2013
National Winner

Pakeman Primary School

Computing - E-Safety Policy

Review Date: February 2018

Next Review Date: February 2020

Ethos Statement

Pakeman School offers a positive, safe learning environment for its community, in which everyone has equal and individual recognition and respect. We celebrate success and are committed to the continuous improvement and fulfilment of potential in every child. We encourage increasing independence and self-discipline amongst the pupils. Everyone within the school has an important role to play in sharing responsibility for the development of positive behaviour and attitudes.

_____ _____

Lynne Gavin
Headteacher

Date

_____ _____

Althea Baker
Chair of Governors

Date

E-Safety covers the use of the internet and different forms of electronic communication (email, mobile phones, forums and social networking). It also relates to the use of cameras and video. It is vital to educate pupils and staff about both the benefits and risks of using technology so that they are able to use computing and ICT equipment safely and effectively.

This policy covers the safe use of computing and ICT equipment at Pakeman Primary School. It is to be used as a reference to ensure that all staff and pupils are aware of important E-safety issues.

1) Aims

The purpose of this policy is to:

- set out the key principles expected of all members of the school with respect to safe and responsible use of computing and ICT-based technologies.
- set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- safeguard and protect children and staff at Pakeman Primary School
- minimise the risk of misplaced or malicious allegations made against adults who work with students.
- have clear structures to deal with online abuse such as cyberbullying, identity theft and grooming.
- protect personal information and to be aware of digital footprints.
- ensure that children and staff are aware of copyright and intellectual property.

2) Roles and Responsibilities:

Headteacher • overall responsibility for e-safety provision and data security • ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • be aware of procedures to be followed in the event of a serious e-safety incident • ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager) • liaise with the Local Authority and relevant agencies
Computing coordinator • establish and review the school e-safety and acceptable use policies • promote an awareness and commitment to e-safety throughout the school • ensure that e-safety education is embedded across the curriculum • liaise with school ICT technical staff • communicate regularly with SLT regarding e-safety issues • ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • ensure that an e-safety incident log is kept up to date. Incidents to be logged on CPOMS

in the relevant section.
Child Protection Officer • report child welfare issues relating to e-safety to the relevant agencies
Teaching and support staff • embed e-safety issues in all aspects of the curriculum and other school activities • supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities) • ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To read, understand and help promote the school's e-safety policies and guidance • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the computing coordinator, child protection officer or headteacher.
Pupils • Read, understand, sign and adhere to the Pupil Acceptable Use Policy (at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • have a good understanding of research skills and the need to avoid plagiarism • understand the importance of reporting abuse, misuse or access to inappropriate materials • know what action to take if they or someone they know feels worried or vulnerable when using online technology. • know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • follow the SMART internet rules

3) E-Safety expectations

- Pupils should be taught about the SMART internet rules (safe, meeting, acceptable, reliable and tell).
- Staff computers should be used for educational purposes.
- Staff and children should all be aware of the risks of viruses and malware, taking educated decisions about websites and programmes that they access.

4) E-Safety awareness

- Termly assemblies are delivered to pupils on e-safety.
- Coffee mornings have been set up to highlight to parents the importance of safe computer and internet use.
- Teachers should refer to e-safety at the start of each computing project or when researching on the internet.
- 'SMART internet use' posters are displayed in all classrooms and e-safety is discussed during annual staff meetings delivered by the computing coordinator.

5) Safeguarding

- All members of staff are expected to read the school e-safety policy.
- Staff and pupils should be aware that internet use can be monitored and traced to the individual user/device.
- Staff members are responsible for the appropriate use of their iPad, computer and class camera.

- Staff that manage filtering systems or monitor computing equipment use will be supervised by senior management and must have clear procedures for reporting issues.
- Staff should report any e-safety issues or concerns to an appropriate member of staff (headteacher, child protection officer or computing coordinator) and record it in the e-safety incident log (kept in the school office).
- Pupils should report any e-safety concerns to their class teacher or an adult that they trust.

6) On-line abuse and cyberbullying

- Pupils are taught that they should not post images or videos of others without their permission.
- We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school.
- We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
- PSHE lessons on cyberbullying should be taught each academic year.

7) Personal information

- Pupils are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Passwords and personal information of staff and pupils should not be shared.
- Pupils should be made aware that personal information posted on social media, in text messages or emails can be potentially accessed and abused by others.
- Staff and pupils should consider their digital footprint and ensure that they are careful in their use of websites.

8) Digital images

- Pupils are advised to be very careful about placing any personal photos on any social online network space.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- Before taking photographs of pupils, staff must ensure that parents or carers have given permission for photographs involving their child (check children's school form if in doubt).

9) Copyright

- Pupils and staff should be aware of 'intellectual property' when using the internet to research information or to access images and video.
- Pupils should be taught to turn their research into their own words rather than copy text directly from websites.