

E-safety Policy

1. Introduction

At St Lawrence C.E.P. School we understand the responsibility we have to educate our pupils on E-Safety issues. We teach them appropriate behaviours and critical thinking skills to enable them to remain safe whilst using the Internet and related technologies, in and beyond the context of the classroom. St Lawrence School has a whole school approach to the safe use of computing and creating this safe learning environment.

This policy has been contributed to by the whole school and ratified by the governors. This policy is to be read in conjunction with all other policies, particularly: Behaviour Policy, Safeguarding / Child Protection Policy, Acceptable Use Policy for Computer Equipment and the Code of Conduct Policy.

School E-Safety training took place in November 2016.

2. Roles and Responsibilities

Paul Dyer (Headteacher) and Emma Dickason (Deputy Headteacher) have overall responsibility and any E-Safety concerns should be passed to them. David Hearn (Senior Leader and Computing Leader) is responsible for keeping abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection), Child Net, Ofsted and N.S.P.C.C. Tim Jackson (Computer Technician) is responsible for ensuring that appropriate restrictions are in place to protect children from unsuitable content.

The Headteacher ensures that the Senior Leadership Team and Governors are updated as necessary.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school E-Safety procedures, particularly by ensuring that:

- E-Safety posters are prominently displayed.
- E-Safety issues are discussed with the children
- Pupils are educated about E-Safety issues – see Computing Scheme of Work

The E-Safety policy will be shared with new staff, including the Acceptable Use Policy for Computer Equipment (AUP) as part of their induction.

3. Curriculum Computing and On-Line Resources

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children. However, there are inappropriate and undesirable elements that must be managed.

- If staff or pupils discover unsuitable sites, the URL (address), time and content will be reported to the teacher who will then report to the Headteacher (or Deputy Headteacher). Inappropriate sites will be blocked by Tim Jackson (Computer Technician).
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will ensure that filtering systems are as effective as possible.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of E-Safety.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an 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.
- E-mail sent to external organisations should be written carefully and authorised before sending
- Chain letters, spam, advertising and all other e-mails from unknown sources will be deleted without opening or forwarding.

Security and Passwords

Passwords are used for some online learning programmes.

- Pupils and staff should never share passwords.
- Staff must not share staff logon with pupils.

Social Networking

Social networking Internet sites 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 are 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 are encouraged to only interact with known friends and family over the Internet and deny access to others.
- Parents, pupils and staff are 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.

Mobile Phones

Mobile phones have access to the Internet and pictures and video messaging. There are risks of mobile bullying and inappropriate contact. Pupils can bring mobile phones onto the school site where it is seen by the school and parents as a safety / precautionary use, for example, if a pupil is walking home alone.

- Mobile phones should be handed in to the class teacher 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.
- 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 can be easily transferred to the Internet.

- Pupils use digital cameras or video equipment under supervision of the class teacher.

- 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.

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.

Reviewed by: Staff & Pupil Welfare Committee
Date reviewed: 18th September 2018
Next review: September 2020