Worplesdon Primary School

E-safety Policy

Target Audience	All staff, governors, parents
Policy Reviewed	November 2017
Reviewed by	ICT Subject Co-ordinator
Next Review	November 2018

Contents

1 Introduction

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as applied to the school's physical environment. This policy document is drawn up to protect the children, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The E-safety Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.

- Our school has a designated E-safety Coordinator, Veronica Bowyer, who is supported by the Designated Safeguarding Leads, Kareen O'Brien (Head Teacher) and Laura Bassett-Cross (Deputy Head).
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-safety Policy and its implementation will be reviewed regularly.
- The E-safety Policy was revised by the Computing Subject Leader and verified by the Senior Management Team, staff and governors.

2 Teaching and Learning

2.1 Why Use The Internet At School?

- The Internet, and related resources, is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children 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.
- Children's learning will be improved through using technologies, such as the Internet, which enhance communication and the sharing of information. The Internet and related technologies also aid the teaching and learning of all subjects across the curriculum, in addition to Computing. Current and emerging technologies which could be used inside or outside of school by children include:
  - the Internet and cloud-based resources;
  - mobile devices, such as laptops and tablets;
  - e-mail;
  - digital video;
  - podcasting.

2.2 The School's Approach to Teaching and Learning Using the Internet and Related Technologies

- E-safety will be taught across the whole school through specific E-safety lessons at the start of each academic year and regularly throughout the academic year thereafter, at least half-termly. Teaching staff have also been advised to identify cross-curricular links and to teach E-Safety as part of other lessons as appropriate.
- Pupils will be taught how to appropriately use and evaluate the Internet and its content, in accordance with the E-safety Programmes of Study in the 2014 Computing Curriculum. Each key phase (FS, KS1, Years 3 and 4, Years 5 and 6) has been given specific and relevant E-Safety planning, complete with learning objectives, success criteria, activity ideas and resource links, to aid delivery of thorough, engaging E-Safety lessons.
- Pupils will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use and learn how to become responsible users of technology.
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- 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 taught how to report unpleasant Internet content.
- It is the teachers' responsibility to supervise access to the Internet and related technologies by checking sites to be used for appropriate content and bookmarking appropriate sites to be used.
- Learners, parents, staff and any other adults will consent to an Acceptable Use Policy Agreement before being allowed Internet access.

3 Managing Internet Access

3.1 Information System Security

- School computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

3.2 E-Mail and Other Electronic Messaging

- Pupils may only use approved e-mail and messaging accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail or message.
- Pupils must not reveal personal details of themselves or others in e-mail or other communication, or arrange to meet anyone without specific permission.
- Staff to pupil e-mail communication must only take place via a school email address, this communication may be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

3.3 Published Content

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. Parents are asked to sign a consent form when their child starts the school and lists of pupils with consent/no consent are available for staff from the school office.
- Parents should be clearly informed, of the school policy on image taking and publishing, both on school and independent electronic repositories.

3.5 Social networking

- The school will control access to social networking sites and consider how to educate pupils in their safe use e.g. use of passwords.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Social networking e-safety information will be available on the school website e-safety page. Pupils will receive regular training as appropriate.

3.6 Managing Filtering

- Access at school is filtered for content appropriate to the age of pupils in the school.
- The school will endeavour to ensure that appropriate protection is in place to protect pupils.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator immediately.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 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.
- Children's mobile phones and associated devices are not permitted: should they be brought into school they must be handed into the school office at the start of the day.

3.8 Protecting Personal Data

- The school shall duly observe all its obligations under the DPA and/or the GDPR.

4 Policy Decisions

4.1 Authorising Internet Access

- All staff must read and agree to the 'Acceptable Use Policy' before using any school Computing resource.
- The school will maintain a current record of all staff and pupils who are granted access to school Computing systems.
- At Key Stage 1, access to the Internet and related technology will be by adult demonstration with directly supervised access to specific, approved on-line materials. At Key Stage 2, children will only be allowed to access Internet sites that have been approved by their teacher.
- Parents will be asked to sign and return an 'Acceptable Use Policy' to demonstrate their acceptance of the Internet practices within the school.
- Any person not directly employed by the school will be asked to sign an 'Acceptable Use Policy' before being allowed to access the internet from the school site. (e.g. trainee teachers)

4.2 Assessing Risks

- 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. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit Computing use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective. This will be done by the Computing Subject Leader, Senior Managers and the E-Safety Co-ordinator through discussions with pupils and staff, monitoring of E-safety lesson planning and delivery, and through annual review of the policy.

4.3 Handling E-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.
- Pupils and parents will be informed of the complaints procedure, which will be available on the school website.
- Pupils and parents will be informed of consequences for pupils misusing the Internet:
  - Any child not conforming to the acceptable use policy (the Internet safety rules displayed in the classroom) will have their Internet use withdrawn.

5 Communications Policy

5.1 Introducing the E-Safety Policy To Pupils

- Appropriate elements of the E-safety policy will be shared with pupils annually at the start of the academic year. E-Safety forms part of the on-going Computing curriculum throughout the year.
- An E-safety Charter will be posted in all networked rooms and all pupils will be asked to sign their names to show that they have agreed to them (Pupils' AUP).This will be done at the beginning of each academic year and pupils will be regularly reminded of the Charter throughout the year.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

5.2 Staff and the E-Safety Policy

- All staff will be given the School E-safety Policy and its 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 computing use will be supervised by senior management and have clear procedures for reporting issues.

5.3 Enlisting Parents' Support

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.