



# **E-Safety and Acceptable User Policy**

Date policy approved and adopted: September 2015

Signed on behalf of the Governors:

Signed by Head Teacher

Date for review: September 2017

## Introduction

This policy has been developed using guidance produced by Oxfordshire County Council and national strategies e.g. Harnessing Technology: Transforming learning and children's services which sets out the government plans for taking a strategic approach to the future development of computing.

The e-Safety Policy will be reviewed annually.

### Teaching and learning

- The purpose of Internet use at Standlake School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management of information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- 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.
- Pupils should be taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact. (DfE Computing Programmes of Study 2014)

### Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data;
- access to learning wherever and whenever convenient.

### The Internet enhancing learning

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### Managing Internet Access

- The security of the school's ICT systems will be reviewed regularly.
- Virus protection is installed and is automatically updated on a daily basis through Sophos.
- The Network manager will review system capacity annually (to coincide with budget planning).
- Specific lessons emphasising internet use and safety issues will form part of a Computing curriculum unit for a period focused around e safety day in the spring term. This is the case from the Foundation Stage to Year 6. Assemblies and whole school activities will form part of this unit of work. Teachers will use their professional judgement to provide reminders and further lessons throughout the year. Direct support is provided to all staff and classes by Nick Speller who is a trained Ambassador for CEOP and as 360 Degree Safe Assessor.

### Published Content – Website

- The website is regularly checked to ensure that there is no content that compromises the safety of the pupils and staff.
- The contact details on the website should be the school's 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.

- The website should comply with Ofsted's requirements and the school's guidelines for publications including respect for intellectual property rights and copyright.
- Pupils' full names will not be used anywhere on the website where they can be matched to a specific photo of the children. Full names may be used in other contexts as long as they do not leave the child vulnerable to contact from an unwanted persons.
- Parents/carers will sign the relevant forms provided if they do not want photographs of pupils published on the school's website.
- Pupil's work can only be published with the permission of the pupil and parents.

### **Social networking and personal publishing**

- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include their photograph, real name, address, phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Teachers are advised not to run social network spaces for pupils on a personal basis or to be in contact with parents from the school on social network sites.
- Standlake School is aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to see the bully's comments.
- The school will work in partnership with parents, the LA safeguarding team, the Department for Education and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to 123ICT who currently manage the filtering system. Any issues with over or under-filtering will be reported to Nick Speller (123ICT) who can remotely update filters.
- In the future pupils may have school email accounts (Office 365).

### **Emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or school time. Staff may use mobile phones in the staff room. Parents and staff may not use mobile phones elsewhere on the premises, in order to meet Safeguarding requirements.
- The sending of abusive or inappropriate text messages is forbidden.

### **Personal data**

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

### **Internet Access**

- The school administrator will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Access to the internet will be supervised.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

### **Risk Assessment**

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.
- Internet filtering is currently provided by ISP (Exa) SurfProtect.

### **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 headteacher.

### **Sanctions**

- Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or exclusion, in accordance with the school's Behaviour Policy. The school reserves the right to report any illegal activities to the appropriate authorities.

### **Communications Policy**

- e-safety guideline posters are posted on the netbook trolley, covering the 4 tips from CEOP for KS1 and the smart rules for KS2.
- Pupils will be informed that Internet use will be monitored. (Potential point for discussion with upper KS2): monitoring v filtering)
- Instruction in responsible and safe use should precede Internet access.
- Sessions on responsible Internet use will be included in the PSHE and Computing programmes covering both school and home use.
- All pupils will read, accept and sign our school e-safety agreement annually (alongside the Home/School Agreement).

### **Employees**

- All staff will be share in the development of the school e-Safety Policy, be made aware of it's importance and sign the Acceptable User Policy.
- Staff should be aware that discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the school's e-Safety Policy will be provided as required.

### **Parental Support**

- Parents' attention will be drawn to the school e-safety Policy in newsletters and on the school Web site.

Policy Agreed .....September 2015

Policy Review Date .....September 2017