Alverthorpe St Paul's CE (VA) School 3-11 years e-safety policy

The e-safety policy relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an e-safety co-ordinator. It is not a technical role.
- Our e-safety policy has been written by the school, building on local authority guidance. It has been agreed by senior management and approved by governors.
- The e-safety policy was revised by: Alistair Lodge
- The next review date is (annually): September 2018

Teaching and learning

Why the Internet and digital communications are important

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.
- A focussed e safety lesson is taught at the beginning of each year, the content of which should be referred to from then on in subsequent lessons.

- Children will make an e safety presentation during either a class assembly or during anti-bullying week.

- Children in Years 5 and 6 will be taught explicitly about cyber bullying.

Managing Internet Access

- School ICT systems security will be reviewed regularly by the ICT Technician/System Administrator.
- Virus protection will be updated regularly by the ICT Technician/System Administrator.
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Unless the author is known, incoming e-mail should be treated as suspicious and attachments not opened.
- The school should consider how e-mail from pupils to external bodies is presented and controlled. The default setting does not enable children to e-mail externally, however we recognise that it is sometimes necessary to enable wider e-mail communication for educational purposes.
- The forwarding of chain letters is not permitted and such emails are discussed with the children as part of their e-safety lessons.

- All internal e-mails are subject to language filters. Any e-mail containing offensive language is automatically blocked and a copy of that e-mail sent to the system administrator. Appropriate action is then taken by the senior management of the school.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The only contact details given online is the telephone number of the school office and school e-mail address of the Head teacher.

- The ICT technician in charge of the website (Mr Sutcliffe) will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils can only be used if written parental consent has been provided.

- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Mr Sutcliffe is responsible for vetting Twitter photos showing images of children. Staff are free to add their own photos of children's work.

Social networking and personal publishing

- The school does not allow access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be advised through their e-safety lessons that the use of social network spaces outside school brings a range of dangers for primary-aged pupils.

Managing filtering

- The ICT Technician/System Administrator will work with the Wakefield authority to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- The ICT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The appropriate use of Learning Platforms is under ongoing discussion.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource.
- The school will maintain a current record of any pupils who are denied access to school ICT systems.
- At Key Stage 1, access to the Internet will directly supervised by an adult.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Wakefield Authority can accept liability for any material accessed, or any consequences of Internet access.
- The school should regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

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 (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Communications

Introducing the e-safety policy to pupils

- e-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- e-safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-safety policy

- All staff will be given the School e-safety Policy and its importance explained at the start of each academic year. Staff sign a code relating to this on an annual basis on an annual basis.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff will always state a clear educational purpose when accessing the web with pupils.

Enlisting parents' and carers' 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.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- The pupil code of conduct for using ICT in school (see appendix A) is to be signed by parents of Foundation/Key Stage 1 children and parents and pupils in Key Stage 2 at the start of each new school year.

Alistair Lodge
E-safety Co-ordinator

Mark Sutcliffe
ICT Technician/
System
Administrator

Christine Chell
Headteacher

Shared with Standards' Committee in October 2017