Sandringham Infant and Nursery School

e- Safety and Acceptable use of IT Policy

Policy Approved	**September 2018**
Review Period	**Annual**
New Review	**September 2019**
Written By	**Laura Theobald**

e-safety and acceptable uses of IT Policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for computing, behaviour and for child protection.

- The school will appoint an e-Safety coordinator.
- 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 annually.

Why 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 students 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.
- The Internet allows pupils to access vast quantities of information that might otherwise be unavailable to them.
- The Internet provides opportunities for pupils to communicate with communities outside their own and learn about the experiences of others.

Internet Use

- The school Internet access is provided by RM and includes filtering appropriate to the age of pupils.
- Pupils will not have unsupervised access to the Internet.
- Internet material derived by staff and pupils will comply with copyright legalities.
- 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 what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will take all reasonable precautions to ensure that the users access only appropriate material.

Information system security

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

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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.
- Staff to pupil email communication must only take place via a school email address and will 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.
- The forwarding of chain letters is not permitted.

Published content and the school web site

The school has a website that provides school policies and information about the school for visitors, diary dates and newsletters for parents. There are also photos that celebrate children's learning and achievements in school.

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils full names are not used anywhere on the website particularly in association with photographs of them.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully. 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 including in blogs, forums or wikis, particularly in association with photographs.
- Parents or carers will have signed the photographic consent form.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking

Social networking sites are commonplace and the school understands that staff, governors, parents and pupils are entitled to access them and post their own information. In accordance with the schools child protection policy, acceptable use of social networking sites means,

- Social networking sites (such as Facebook) are not to be used by either adults or children at school.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Staff, governors and parents do not post inappropriate or damaging material about the school, pupils or parents on social networking sites.
- Photographs of children that have been taken in school or on school educational visits are not posted on social networking sites.
- Staff will not comment on posts about children.

Managing filtering

- The school will work in partnership with RM 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.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing other technologies

- All technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the wii and Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use.
- Staff will use a school phone where contact with pupils is required.

- The school reserves the right to confiscate 4G/mobile technology if staff believe it could be used inappropriately. This will be returned by a member of SLT to a parent/guardian.

Managing Data Security

In order to function, schools must hold personal data on learners, staff and other people. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. This loss of sensitive information can result in media coverage and potentially damage the reputation of the school.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and should be made aware of the risks and threats and how to minimise them.

Acceptable use of data means:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Parents must be asked permission before any videos or photographs are used in publication or displayed by the school in a public place. Careful liaison with parents is essential particularly when a parent does not agree to their child being photographed. Staff must make every effort to comply with sensitivity. After discussion it may be possible to agree other options e.g. a team photograph without names.
- When photographs are to be used or taken by the press, the newspaper will be asked not to use the child's name. However if the child's image is with their name attached consent should be obtained.

Photographs in School

At Sandringham, photographs and videos of children and their work form an important part of teaching, learning and record keeping. Acceptable use of photographs that protects children, staff and parents means,

- Photographs of children will be taken only on cameras or memory cards not mobile phones.
- Photographs of children will only be stored on the school's network, school laptops or encrypted memory sticks.
- Parents and carers working in school or helping on educational visits will not take photographs of children using their own cameras or mobile phones.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs or videos for their own personal use, the school will demonstrate their protective ethos by announcing that photographs taken are for private retention and not for publication in any manner including use on personal websites or social networking sites. (Such as Facebook)

Portable data storage

Every teacher in school will be supplied with an encrypted memory stick to support teaching and record keeping. Acceptable use of portable data means;

- School memory sticks will be used for the storage of planning, resources and assessment.
- School information including photographs will not be stored on personal memory sticks or laptops.
- Teachers will take reasonable precautions to ensure that school memory sticks are not infected with viruses or malicious software when used at home.

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school IT 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 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 IT 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.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school e-safety policy.

Communications Policy

- Introducing the e-safety policy to pupils
- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- 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.

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 ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school prospectus and on the school web site.
- Parents and carers will from time to time be provided with additional information on e-safety.
- Pupils will not be granted access to the Learning Platform until a parent/guardian has attended an e-learning meeting in school.