Sandiway Primary School

Online Safety policy

December 2021

Our online safety policy has been developed by a working group made up of Mrs C Forsyth (Computing Lead) and the Headteacher.

Aims

At Sandiway Primary School, we recognise that computing and the use of the internet plays an important role in children's learning. Sandiway Primary School believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles. Sandiway Primary School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

The purpose of this policy is to:

- Identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Sandiway Primary School is a safe and secure environment.
- Safeguard and protect all members of Sandiway Primary School community online.
- Raise awareness regarding the potential risks as well as benefits of technology
- To enable all staff to work safely and responsibly, to be a role model for positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff who work for or provide services on behalf of the school, as well as children and parents/carers. This policy applies to all access to the internet and use of ICT devices including personal devices or where children, staff or other individuals have been provided with school devices for use off-site, such as a work laptop or mobile phone. This policy must be read in conjunction with other relevant school policies. (BYOD Policy, Acceptable Use Policy, Safeguarding Policy)

Key Principles

Why Internet use is important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- We have a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in the school is to raise educational standards, to promote pupil achievement, to support the professional work of all staff and to enhance the school's management functions.

How can Internet use enhance learning?

- Pupils will be taught what Internet use is acceptable and what is not and will have clear objectives for Internet use.

- Access levels to the internet to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and information.
- Pupils will be taught to acknowledge the source of information used and to respect copywriting when using Internet material in their own work.

How will Internet access be authorised?

- School will maintain a current record of all staff and pupils who are granted access to the schools electronic communications.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- At Sandiway Primary School, pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use. This will be undertaken in Computing, PSHE lessons and assemblies.
- E-safety posters are displayed in each classroom and these are referred to frequently demonstrating clear rules for online safety.

Students will be taught how to evaluate Internet content and share concerns.

- We will ensure that the use of Internet derived materials by staff and students complies with copyright law.
- Through our computing, and PSHE lessons, our students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to share any concerns about internet content with their teacher.
- Cyber-bullying is addressed through PSHE, assemblies and discrete computing lessons. Children are taught to share any incidents of cyber-bullying with an adult, such as their parent/carer, their teacher or a teaching assistant should they feel that they are being bullied, threatened or intimidated whilst using the Internet or mobile devices.

E-mail

- Our students only use an approved e-mail account on the school system for their class.
- Pupils are taught to immediately tell a teacher if they receive an offensive e-mail or message.
- Through e-safety lessons, children at Sandiway Primary School are taught not to reveal personal details of themselves or others in e-mail communication, not to open messages from unknown parties, and not to arrange to meet anyone without specific permission.

Responding to Online Incidents and Concerns

- All members of the school/setting will be informed about the procedures for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content)
- The safeguarding lead will ensure that online safety concerns are escalated and reported to relevant agencies in line with school policy.
- Complaints about Internet misuse will be dealt with under the school's complaints procedures.
- Complaints about online bullying will be dealt with under the schools bullying policy
- Any complaint about staff misuse will be referred to the Headteacher
- Any allegations against a member of staffs online conduct will be discussed with the Headteacher
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Published content and the School website

- The contact details on our school website are the school address, e-mail, and telephone number.
- Staff or pupils personal information is not published.

- The Headteacher takes overall editorial responsibility for the website and ensures that content is accurate and appropriate.

Publishing students' images and work

- Pupils full names will not be used anywhere on the website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/blog.
- Pupils work can only be published with the permission of the parents
- Parents and carers may take photographs at school events, but these may not be shared publicly through social media sites such as Facebook.

Social networking and personal publishing

Sandiway Primary School has a managed ICT maintenance service provided by an outside contractor, Redtop. School's Broadband provides the broadband connection and filtering of the internet, which is in turn managed by Redtop It is the responsibility of Sandiway Primary School to ensure that the managed service provider carries out all the online safety measures that would be otherwise be the responsibility of the school technical staff. The online policy has been shared with the managed service provider.

Redtop is responsible for;

- The schools infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements.
- Filtering is applied and updated on a regular basis.
- The use of the network is regularly monitored in order that any misuse can be reported to the Headteacher for investigation.
- Monitoring software is implemented and updated as agreed in school, this is done through School's Broadband who provide the filter
- The school and School's Broadband block access to social networking sites, other than those approved – Twitter and YouTube.
- Pupils are routinely told never to give out personal details of any kind which may identify them or their location, nor to accept 'friend requests', nor respond to other messages from unknown parties, and to report these where appropriate.
- Pupils are made aware of the dangers of social network spaces and how to minimise the risk.

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 following BYOD Policy.
- Mobile phones are not permitted for use by pupils in school. Where pupils need to bring them in, for after school events etc, they must be left with class teachers and switched off.
- Staff must not use their mobile phones in the presence of pupils other than for 'school business', Tweeting, etc.
- Pupils and their parents accept full responsibility for any personal 'devices' which they choose to bring into School to assist them with their work.
- Staff will use a school phone, their school email address, or the school's text system where contact with students, parents or outside agencies is required.
- Staff and pupils should only use their own login details. Usernames and passwords should not be shared with others.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR.

Policy Decisions

Authorising Internet access

- All staff must read the Online Safety Policy

- The school will keep a record of all staff 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.

Assessing risks

- 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. Neither the school nor Redtop can accept liability for the material accessed, or any consequences of Internet access.
- The School will audit Computing provision to establish if the Online Safety Policy is adequate and that its implementation is 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 safeguarding nature must be dealt with in accordance with school safeguarding procedures.

Communications Policy

Introducing the Online Safety Policy to pupils

- E-Safety rules will be posted in classrooms and discussed with the pupils at the start of each year.
- Pupils will be reminded of the e-Safety rules at the beginning of each half term.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be educated in safe Internet use in the home.
- The school will send parents literature so they can use the Internet safely at home.
- Parents will have the opportunity to discuss any concerns with a member of staff

Staff and the e-Safety Policy

Staff are responsible for ensuring that;

- An up to date awareness of online safety matters and of the current school Online safety Policy and practice
- They have read and understood and signed the Staff Acceptable Use Policy.
- Report any suspected misuse or problem to the Headteacher for investigation.
- All digital communications with parents should be on a professional level and carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities
- 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.

Enlisting parents’ support

Parents’ attention will be drawn to the school e-Safety policy in newsletters, the school newsletters and on the school website.

Responsibility of Local Academy Board (LAB)

- The LAB is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Regular information about online safety incidents and monitoring reports will be regularly updated. A member of the LAB will take on the role of safeguarding member.
- The LAB is responsible for the approval of the e-Safety policy, for ensuring that there is a clear strategy for e-Safety, and for reviewing the effectiveness of the policy through regular reports on e-Safety incidents
- The LAB will ensure that the e-Safety policy is reviewed regularly in the light of technological developments

Date Reviewed – December 2021

Date for Review - December 2023