Sandhill Primary School
e-Safety Policy
December 2020

Introduction

E-Safety encompasses internet technologies and electronic communications including mobile phones, mobile and wireless technology.
The statutory curriculum requires children to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This use is achieved across a wide variety of technological platforms. It brings children into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. Our policy highlights the need to educate children about the benefits and risks of using various technologies and provides safeguards and awareness for users to enable them to control their online experiences.

This e-Safety Policy, built on five core principles, provides overarching guidance to safeguard our children. It operates in conjunction with other school policies identified in the Appendix.

Core Principles of Internet Safety

Guided Educational Use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and carefully managed environment. Directed and successful Internet use will also reduce the opportunities for children to get to the 'wrong place'.

Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become 'Internet Wise'. At Sandhill it is our responsibility to ensure that the children are fully aware of the risks, perform risk assessments and implement an effective policy for Internet use. Our children need to know how to cope if they come across inappropriate material.

Responsibility

Internet safety depends on all staff in school, parents and, where appropriate, the children themselves taking responsibility for the use of Internet and other communication technologies. The balance between educating children to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation

The use of a finite and expensive resource, which inevitably brings with it the possibility of misuse, requires regulation. In some cases, access within our school will be denied, for instance un-moderated chat rooms. Fair rules, clarified by discussion and prominently displayed at the point of access will help children make responsible decisions. At Sandhill various levels of access rights will be determined and actioned by our ECM ICT Technical Team in discussion with the Headteacher. Blocking and the unblocking of sites will be at the discretion of the Headteacher.

Appropriate strategies

This policy describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding children towards educational activities. Strategies must be selected to suit each situation with their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the children themselves must remain vigilant

Purpose and scope of this policy

- The purpose of Internet use in school is to raise educational standards, to promote children's achievement, to support the professional work of staff and to enhance our management information and business administration systems.
- Internet access is an entitlement for our children who are expected to show a responsible and approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. It is our responsibility to provide children with quality Internet access as part of their learning experience.

E-safety depends on effective practice at a number of levels

- Responsible ICT use by all staff and children; encouraged by education and ongoing awareness raising and made explicit through our published policies.
- Support and guidance for parents, giving them the knowledge and confidence to be able to supervise their child's use of digital and interactive technology.
- Sound implementation of our e-safety policy in both administration and raising awareness, including secure network design and use.
- Safe and secure broadband access incorporating appropriate firewalls and the effective management of content filtering network standards and specifications.

How will Internet use enhance learning at Sandhill Primary?

- Our Internet access is designed expressly for the use of the children and includes filtering appropriate to their ages.
- Children will be taught what Internet use is acceptable and what is not and given clear guidance and training on Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide the children's on-line activities that will support the learning outcomes planned.

- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- At our school we maintain a current record of all staff and children who are granted internet access.
- All staff are expected to read and sign to say they accept the E-Safety and Acceptable Use Agreement before using our ICT equipment and resources.
- Parents / carers are informed that children and young people will be provided with supervised internet access and are asked to sign and return a consent form for children's access. This is completed as part of our admissions to school process and reviewed periodically.

Email

- School can and may monitor my use of Computing and ICT systems, email and other digital communications.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on organisation headed paper.
- Children, young people and their families should only contact members of staff using school email addresses or telephone numbers. This includes staff who they knew before joining Sandhill Primary. Any exceptions to this should be discussed with the Headteacher. This is to safeguard the children, their families and the member of staff from potential allegations of misconduct.

Social Networking
See our Social Networking Policy

Blogging
See our Blogging Policy

Filtering

- We work in partnership with our Technical Team to ensure filtering systems are as effective as possible in order to protect all users. Various levels of user account are managed and monitored internally.
- Filtering strategies are selected by our Technical Team after discussion with senior staff. The filtering strategy will be selected to suit the age and curriculum requirements of the children.
- Any breaches of the filtering system are to be reported immediately via the agreed procedures. This should be reported in the first instant to the Headteacher.
- Any material that we believe is illegal will be referred to the Internet Watch Foundation and CEOP as a matter of course.

Video Conferencing

- Children using video-conferencing will be appropriately supervised.

Information System Security

- Our ICT Technician will review the ICT systems capacity and security regularly and report to the appropriate persons.
- Virus protection will be installed and updated regularly.
- Security strategies should be discussed with the senior management team and shared with all users.
- Use of portable media such as encrypted memory sticks will be reviewed on a regular basis. Portable media may not be brought into school without specific permission and a full virus check.
- Files held on our network will be regularly checked by our Technical Team who will also ensure that the system has the capacity to take increased traffic caused by Internet use and that the system is fully maintained.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Use of Digital and Video Images - Photographic, Video

- The development of digital imaging technologies has created significant benefits to learning, allowing children instant use of images that children or staff have recorded themselves or downloaded from the internet.
- However, staff / children need to be aware of the risks associated with sharing images and with posting digital images on the internet.
- Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is worth noting there are an increasing number of reported incidents of employers carrying out internet searches for information about potential and existing employees.
- The school will inform and educate users about these risks and will implement protocols to reduce the likelihood of the potential for harm.
- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow the policy concerning the sharing, distribution and publication of those images.
- Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's names will not be used anywhere on a website or blog.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website or indeed anywhere else.

Published Content and our Web Site

- The contact details on the website will be the address, e-mail and telephone number of the school.
- Personal information about staff, including volunteers, children, young people or their families should not be published, except where it is required to meet website compliance guidelines e.g. Governor information.
- The Headteacher and ICT team have overall editorial responsibility and ensure that content is accurate and appropriate.

Managing other Technologies

- Emerging technologies will be examined for educational and developmental benefit and a risk assessment will be carried out before use is considered.
- Children should not use mobile phones in school.
- Staff should not use their personal mobile phone to contact children, young people or their families. Where this is necessary the school mobile must be used.

Assessing Risk

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international access available via the internet, it is not possible to guarantee that unsuitable material will never appear on our system.
- Any child, young person or member of staff who inadvertently accesses inappropriate sites or materials should immediately report the incident to the Headteacher.
- As an ongoing process we will audit ICT use to establish if the e-safety policy is successful and that the implementation of the e-safety policy is appropriate.
- School computers should not be available to anyone outside of normal working hours other than for authorised staff and supervised children.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling E-safety Complaints

- Responsibility for handling incidents will initially be assessed by the nominated Technician. For minor breaches of our ICT Policies children will be dealt with in accordance with the school policies. For more serious breaches of e-safety the matter will be referred to the senior member

of staff who will decide upon the appropriate course of action consistent with the Behavior Policy.
- Any complaint about staff misuse must be referred to the Headteacher as a matter of course.

Roles and Responsibilities –

Teaching and non-teaching staff must ensure that

- They have an up to date awareness of e-safety matters and of the current school policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the appropriate senior staff.
- All digital communications with children must be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Children understand and follow the school e-safety and acceptable use policy.
- Children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons and in after school activities where appropriate.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Children should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Parents and Carers

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.
- Research shows that some parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore support parents by providing information and offering appropriate training and advice.
- Parents and carers will be responsible for endorsing (by signature) our Pupil Acceptable Use Policy

E-Safety education will be provided in the following ways -

To Children

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. This will include participating in national and local e-safety events as appropriate.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Children should be helped to understand the need for the children's AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

To Teaching and Non-teaching Staff

- All staff, including new staff, will be given access to a copy of this policy, its importance explained and asked to sign the User Agreements in place.
- Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The Headteacher will receive regular updates on e-safety as appropriate.
- E-safety training will be made available to staff where necessary.

Appendix

Other policies which relate to this E-Safety Policy include -

The Blogging Policy
The Social Networking Policy
The Computer Information Security Policy
The Acceptable User Agreement for Internet and Email
General Data Protection Regulation Policy (Data Protection Policy)

E-Safety rules from FS to Y6

Foundation Stage – Think then Click

These rules help us to stay safe on the internet

1. We only use the internet when an adult is with us
2. We can click on the buttons when we know what they do.
3. We can search the internet with an adult.

Key Stage 1 - Think then Click

These rules help us to stay safe on the internet

1. We only use the internet when an adult is with us
2. We can click on the buttons when we know what they do.
3. We can search the internet with an adult.
4. We always ask if we get lost on the internet.
5. We can send and open emails together.
6. We can write polite and friendly emails to people that we know.

E-Safety Rules for Key Stage 2

1. We ask permission before using the internet.
2. We tell an adult if we see anything we are uncomfortable with.
3. We immediately close any webpage we not sure about.
4. We only e-mail people an adult has approved.
5. We send e-mails that are polite and friendly.
6. We never give out personal information or passwords.
7. We never arrange to meet anyone we don’t know.
8. We do not open e-mails sent by anyone we don’t know.
9. We do not use Internet chat rooms.

This policy will be reviewed on an annual basis or sooner if more guidance becomes available.

Signed ______________________ Headteacher

Signed ______________________ Chair of Governors