STRAIDHAVERN PRIMARY SCHOOL

E-Safety POLICY

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

In ***Straidhavern Primary*** we understand the responsibility to educate our pupils in Online Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key Concerns are:

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons

Children should be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details or
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content. Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.
Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught:-

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. *Teachers, pupils and parents must be vigilant.*

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator (Miss Mc Kenzie) to keep abreast of current Online Safety issues and guidance through organisations such as C2k and the UK Safer Internet Centre. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of Online Safety throughout the school.

The Principal/ ICT Co-ordinator update staff and Governors with regard to Online Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the Online Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection and Safe Guarding, and Anti-bullying.

It has been agreed by the Principal, Staff and approved by the Governing Body. The Online Safety policy and its implementation will be reviewed annually.

Online Safety Skills' Development for Staff

- All staff receive regular information and training on Online Safety issues through the co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate Online Safety activities and awareness within their lessons.

Online Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website and other platforms.
- The school website contains information and links to useful sites
- **The school will communicate relevant Online Safety information through newsletters, Class Dojo and the school website.**

Parents should remember that it is important to promote Online Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach Online Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as C2k / Uk Safer Internet Centre.
- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- 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.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

- Pupils may only use C2k e-mail and straidhavernps.co.uk accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must be cautious about revealing personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

- The school C2k system will block access to social networking sites. Pupils in Key Stage Two will have access to Google Hangouts/Meet for the purpose of global collaboration.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should be cautious when storing information and photographs on portable memory devices.
- Pupils are not allowed to use personal mobile devices/phones (in school) during class.
- Staff should not use personal mobile phones during designated teaching sessions unless being directly used for educational purposes.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website and social media platforms. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the School Website or social media platforms, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's Online Safety rules. These Online Safety rules will also be displayed clearly in all rooms.

- Access to the Internet will be supervised.

- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's Online Safety rules and within the constraints detailed in the school's Online Safety policy.

- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling Online Safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the Online Safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal.
- 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.

Communicating the Policy:

Introducing the Online Safety Policy to pupils

- Online Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons, circle times, anti-bullying week, internet-safety week.
- Pupils will be informed that network and Internet use will be monitored**.**

Staff and the Online Safety Policy:

- All staff will be given the School Online Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A technology hardware devices issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Monitoring and review:

Staff access to modules in SIMS (Schools Information Management System) is approved and monitored by the Principal.

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator (Miss Mc Kenzie)

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

Safety Rules for Children

Follow These SMART TIPS

S

Safe – keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number or password.

M

Meeting – Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them a long time.

A

Accepting- emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems-they may contain viruses or nasty messages!

R

Reliable Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T

Tell – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

www.kidssmart.org www.childnet.com