Swinemoor Primary School

Acceptable Internet Use Policy

This policy should be read in conjunction with the following policies: E Safety Policy, Data Protection Policy

Swinemoor Primary School will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used if parental consent has been given

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in for education, business and social interaction. The school has a duty to provide all students with quality Internet access as part of their learning experience.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfES.

How will Internet use 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 is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-coordinator.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

How will e-mail be managed?

- Pupils 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 details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Whole-class or group e-mail addresses should be used.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- The headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Are newsgroups and chat safe?

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. The importance of chat room safety will be emphasized.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

How can emerging Internet uses be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

How will Internet access be authorised?

- Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 ERYC can accept liability for the material accessed, or any consequences of Internet access.
- 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.
- The headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

How will filtering be managed?

- The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-coordinator.
- The Internet Service Provider also provides a system to filter unsuitable material. Any material which escapes the filter will be reported to the ISP immediately.

How will the policy be introduced to pupils?

- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will precede Internet access.

How will staff be consulted?

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is utilised.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal software may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.

September 2018

Swinemoor Primary School

Responsible Internet Use

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- **I will ask permission before entering any Web site, unless my teacher has already approved that site.**
- **I will not look at or delete other people's files.**
- **I will not bring software into school without permission.**
- **I will only e-mail people whom my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **I will not use social media in school.**
- **I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I know that the school may check my computer files and may monitor the Internet sites I visit.**
- **I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.**

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

All personal data held on the school's network is subject to the Data Protection Act 1998 (and subsequently the General Data Protection Regulation (GDPR) and the school's Data Protection Policy.

Safety in a Digital World: Guide for Children and Young People

Digital technology opens up a world of entertainment, opportunity and knowledge. To help you stay safe this guide aims to provide information on:

- The benefits of Digital Technology
- Addressing the risks
- Further advice and support

The safety advice below applies to all digital technology including computers, mobile phones, TVs, iPods, mass storage devices *etc*.

The Benefits of Digital Technology

You can use digital technology for many reasons, including:

Finding and sharing information – Researching topics on the internet, for school, college and for personal interests, and sharing media like files, pictures, films and music.

Keeping in touch with family and friends – Staying in touch with family and friends through: Email, Instant Messaging (IM), Social Networking and chat rooms technology can be useful for contacting people in an emergency and making new friends in a safe way.

Entertainment – Listening to music, watching films, and playing interactive games.

Shopping – Buying items from companies and individuals all over the world, including online auctions.

Addressing the risks: Digital technology agreement:

There are however some risks in using digital technology – follow this advice and sign this agreement to help keep you safe.

I agree to keep my personal information safe

Be careful what information you put on the internet and who can see it. Use a nickname online and privacy settings. This can help keep you safe.
Don't give out personal information like email addresses, home or school addresses or mobile phone numbers to people you do not know.
Only post photographs which you would be happy with your parents/carers seeing and make sure they don't show addresses. Photographs you post can be copied and sent to other people meaning you are not in control of them.
Do not share your passwords and log in details as people could access your information without your permission.

I will tell adults about the sites that I am worried about.

I agree not to meet people without asking a parent/carer/adult.

Some people on the internet are not who they say they are. Be careful who you chat to and make friends with on Social Networking sites like Facebook, Instagram and Snapchat. Never agree to meet someone without letting an adult know.

I agree to report and worries I have to an adult.

If anyone online makes you worried or says things that make you feel uncomfortable tell an adult or click 'Report abuse' button (some websites will ask you to download this first) and block them.
Do not respond to upsetting messages and cyber-bullying. Keep the message and show it to an adult you trust.

I agree not to use digital technology to bully people or make threats.

Cyberbullying is not acceptable and can cause distress.
Treat people as they would like to be treated.

Signed..... Date.....

Further advice and support:
If you want to find out more about using digital technology safely go to:
www.thinkyouknow.co.uk Digital safety advice
www.ceop.gov.uk Report Abuse Button

Remember the internet safety code. Click Clever, Click Safe

- **Zip It** – Keep your personal stuff private and think about what you say and do online .
- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments.
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.

Safety in a Digital World: Guide for Professionals

Technology is provided and maintained for the benefit of all staff within Swinemoor Primary School to enhance skills and become more effective in the workplace. You are encouraged to use and enjoy these resources, using the following agreement as a guide.

There is a need to ensure that digital technologies are used appropriately and for you to have an understanding of your responsibilities in keeping yourself and young people safe. This guide aims to assist you, making sure that you have all necessary measures in place.

Internet and Email

- **I agree to only access suitable material**;
  I am aware that accessing materials which are unlawful, obscene or abusive is not permitted.
- **I agree to report unsuitable material;**
  If I receive an email containing material of a violent, dangerous, racist, or inappropriate content, I will always report such messages to the E-safety Co-ordinator.
- **I agree to the professional code of behaviour;**
  I appreciate that other users might have different views from my own and acknowledge that the use of strong language or aggressive behaviour is not acceptable.
- **I agree to keep within copyright laws;**
  I will respect work and ownership rights of people, including abiding by copyright laws.
- **I agree to the responsible use of social networks, both within and outside the workplace;**
  The use of social networks for personal communication with children and young people for whom I am responsible is not appropriate.

Equipment

- **I agree to take care to protect hardware and software;**
  This includes protecting the ICT equipment from spillages by eating or drinking well away from them. I will always get permission before installing, attempting to install or storing programs of any type on the ICT equipment. I will always check files brought in on removable media (such as CDs, flash drives *etc*) and mobile equipment (*e.g.,* laptops, PDAs *etc*) with antivirus software and only use them if they are found to be clean of viruses. I will only open attachments to emails if they come from someone I already know and trust. I understand that attachments can contain viruses or other programs that could damage files or software.
- **I agree to only using equipment within the context of my professional role;**
  I will only use ICT equipment for Swinemoor Primary School purposes. I understand that activities such as buying or selling goods are inappropriate.

Security and Privacy

- **I agree to take measures to protect access to data;**
  I will keep my log-on user name and password private, **always log off when I have finished working or am leaving the ICT equipment unattended**. I am aware that I must never use someone else's user name. To protect myself and the systems, I will respect the security on the ICT equipment; I understand that attempting to bypass or alter the settings may put my work or other people's information at risk. I will not send sensitive information via FAX or non-secure email.

Mobile phones

- **I agree to always abide by Swinemoor Primary School policy for use of mobiles in the workplace;** I understand that the use of mobile phones for personal communication with children and young people for whom staff/volunteers have responsibility is not appropriate. Any such contact should be with the express permission of the Headteacher and recorded.

Name (print)……Signed……..……

Swinemoor Primary School

Date ……..……