Five Ways Primary School

E-Safety Policy

September 2016

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy operates in conjunction with other policies including those for Safeguarding, Behaviour and Discipline, Anti-Bullying, Curriculum, Data Protection and Security.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Internet for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

Availability of Policy

The policy is available to staff in each staff room in the appropriate policy folder. It is also available electronically in the Staff area of the network. Parents can access the policy on the website.

Contents

School e-Safety Policy

The e-Safety team consists of:

- Mrs R Mander (Headteacher, Designated Safeguarding Lead)
- Mrs S Fuller (Deputy Headteacher, Designated Safeguarding Lead)
- Mrs L Langston, Miss J Grice (ICT Leaders/ E-Safety)
- Mr K Mullally (ICT Team)
- Mr M Birch (Nominated Governor for Safeguarding/ E-Safety)

Roles and Responsibilities

Name	Role	E-safety Responsibility
Mrs Rachel Mander	Headteacher	To ensure that the school meets all statutory requirements in relation to e-safety. To ensure all staff are equipped with the necessary skills to be able to undertake their role effectively.
Mrs Sue Fuller	Deputy Headteacher	To oversee the work of e-safety team. To deal with any issues arising, liaising with staff, pupils, parents, LA, outside agencies as required.
Mrs Leanne Langston Miss Jade Grice	ICT Leaders/ E-Safety	To lead on E-Safety across the school in liaison with SLT.
Mr Kevin Mullally	ICT Team	To monitor whole school computer use with security software. To inform SLT of any issues arising. To review and advise staff on policies and procedures related to e-safety. To deliver the e-safety message through ICT lessons.
Mr Mark Birch	Nominated governor for safeguarding/ E-Safety	To evaluate the work of the e-safety team. To ensure that school is meeting statutory requirements related to e-safety and safeguarding of children.

It is recognised that all staff, parents and pupils also have a responsibility related to e-safety. Staff must supervise children when using ICT equipment and report any issues to the e-safety team. Parents need to discuss internet use with their children and sign a permission slip if they wish their child to use the internet in school. Parents are also encouraged to monitor their child's computer use at home. Pupils are taught to use ICT equipment safely and understand that they have a responsibility to follow the rules.

Our e-Safety Policy has been agreed by this team and approved by the governing body.

The e-Safety Policy is reviewed annually. This policy will next be reviewed September 2017.

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 administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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, retrieval and evaluation.

Authorised Internet Access

The school maintains a current record of all staff and pupils who are granted Internet access. This is kept in the school office and maintained by Mrs W Russell.

- All staff must read and sign the 'Acceptable ICT Use Agreement', on an annual basis, before using any school ICT resource. Copies of these are kept by the E-safety leader and in the school office, to be maintained by Mrs W Russell.
- Upon entering Year 2, all parents are informed that pupils will be provided with supervised Internet access and are asked to sign and return a consent form for their child(ren). Copies are to be sent to the school office and permission will be included on Sims.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- If the site is deemed to be of a serious nature, the member of staff supervising the lesson must remove the power supply to that particular computer. The computer must be clearly labelled as out of use and the e-safety coordinating team informed immediately. The team must then contact the Local Authority helpdesk. The computer must remain switched off during this process. The head teacher will also be informed and the matter will be discussed with parents where appropriate.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- 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 personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to pupils' external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully as everything sent from Five Ways is a representation from the school.
- The forwarding of chain letters is not permitted.

Scratch

- Children from Year 2 onwards will be using Scratch as an internet based program. The children will be encouraged to use this program at home to enhance and add to their school projects. This program gives the children the opportunity to chat online; as such we will need to make parents aware of this facility and to gain their permission.

Social Networking

- We have blocked access to social networking sites and newsgroups.
- As part of their ICT lessons pupils are taught:
    - never to give out personal details of any kind which may identify them or their location
    - not to place personal photos on any social network space.
    - to set passwords, deny access to unknown individuals and how to block unwanted communications.
    - to invite known friends only and deny access to others.

Filtering

The school uses RM's Internet for Learning service which is filtered at local authority level. We have local control over this and can block sites which we consider inappropriate or unblock sites that we feel should be allowed. Securus is also installed on the network which monitors pupil and staff access.

Policy Central Enterprise

If violations are discovered during the monitoring process, the following procedures must be observed.

- Monitoring will be carried out on a weekly basis by Kevin Mullally.

- **'Save as flagged'** any content which may be deemed as a cause for concern.

- Where deemed as a violation then the pupil, class teacher and ICT teacher must be identified. Record on relevant form. Headteacher to be informed.

- ICT teacher and Year Leader to give verbal warning to the pupil and parents to be informed.

- If a second violation occurs then the restriction of internet access must be considered.

Managing Emerging Technologies

- Staff will be aware of the confidential nature of data that may be held on personal ICT equipment and will act accordingly.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.
- If laptops are taken off the premises, confidential information must be password protected and only used by the person with responsibility for the information.
- Memory sticks or other electronic storage devices which contain sensitive information must also be password protected.
- It is recommended that staff use school iPads to take pictures of the children. Personal cameras or other equipment must treat images as confidential and delete data after use.
- Many staff are choosing to save lesson plans and resources on Web based sites (such as Sky Drive) rather than using a memory stick. These must be UK based and password protected. Sensitive data must still be saved onto memory sticks.

Published Content and the School Web Site

- The contact details on the Web site consist only of the school address, e-mail and telephone number. Staff or pupils personal information is not published.
- The Website is currently updated by Alison Fletcher (Office) and the PTFA.

Publishing Pupils' Images and Work

- Photographs that include pupils are selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website or any other school web presence.
- Written permission from parents or carers is always obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.
- Any photographs of children taken by staff must be treated confidentially and must only be used for display purposes. Images must be deleted after use.

Information System Security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies are regularly discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

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. We have robust filtering and monitoring systems in place. However neither the school nor Staffordshire Local Authority can accept liability for the material accessed, or any consequences of Internet access.
- The school regularly audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a member of the senior leadership team. The head teacher should always be informed. Then the complaint needs to be referred to the county LADO if necessary.

Communication of Policy

Pupils

- Rules for Internet access are posted in all networked rooms.
- All pupils are informed that Internet use will be monitored.
- Pupils read Email and Internet Use Rules with parents.

Staff

- All staff are made aware of the School e-Safety Policy and its importance.

- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff sign a ICT Use Staff Declaration form annually.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Email and Internet Use Rules to be read and signed by parents.

Internet and Email Rules and Agreements for Staff

	Notes	ICT Security Policy Paragraph Reference
1.	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.	4.5.1
2.	You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 The Telecommunications Act 1984 provisions of this legislation may result in disciplinary, civil and/or criminal action.	5.1.2
3.	ICT resources are valuable and the confidentiality, integrity; availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held.	5.2.2, 6.2, 6.3 & 6.4
4.	Follow the local rules determined by the Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the System Manager.	5.4.4 & 8.2.1
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave you computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.	7.2.1
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the System Manager.	8.4.1

7.	The System Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a “made up” word, but not obvious or guessable, e.g. surname; date of birth. Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the System Manager, e.g. in cases of shared access. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle/drawer to which only you have access.	8.6.1
8.	The System Manager will advise you on what “back ups” you need to make of the data and programs you use and the regularity and security of those backups.	8.7.1
9.	Ensure that newly received floppy disks, CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the System Manager.	8.8.1 & 8.8.2
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, floppy disks, etc.	8.9.1
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Headteacher, Chair of Governors or Internal Audit.	9.1
12.	Users of these facilities must complete the declaration attached to the “E-mail & Internet Acceptable Use Policy”.	10.1

Staff Guidelines E-mail & Internet Use Good Practice

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet E-mail services.

You should:

- check your E-mail inbox for new messages regularly;
- treat E-mail as you would a letter, remember they can be forwarded / copied to others;
- check the message and think how the person may react to it before you send it;
- make sure you use correct and up to date E-mail addresses;
- file mail when you have dealt with it and delete any items that you do not need to keep;

You should not:

- use E-mail to manage staff where face-to-face discussion is more appropriate;
- create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- print out messages you receive unless you need a hard copy;
- send large file attachments to E-mails to many addressees;
- send an E-mail that the person who receives it may think is a waste of resources;
- use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.

ICT Use - Staff Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the School's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users - Staff, and the conditions in the E-mail and Internet use policy, including those in the 'E-mail & Internet Use Good Practice'.

I have read the E-safety policy and I am aware that my use of ICT will be monitored.

Your details

Name:

Job title:

Signature: Date: