

Safeguarding- **E-Safety and Acceptable Use Policy** and Guidelines (Reviewed September 2019)

Background

Many of our pupils interact with new technologies such as mobile phones, tablets and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

This policy is aimed at helping us think about the responsible use of ICT and to decide on the right balance between controlling access, setting rules and educating students for responsible use. This policy should be part of an overall approach which includes discussions with parents and carers at home.

This policy considers all aspects of e-safety, which encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It will be regularly reviewed in the light of any new or emerging technologies that might impact on our children's learning.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

This policy aims to make it clear to staff, pupils and visitors that it is unacceptable to use the school equipment for inappropriate reasons and we need to ensure that all reasonable actions have been taken and measures put in place to protect users. It has been written by the school, building on the national schools E-Safety guidance. It has been agreed by the senior management and approved by governors.

What technologies does this policy cover?

This e-safety policy considers the use of both fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, tablets and portable media players. It includes guidance on Internet searching, email, instant messaging, chat rooms, social networking sites and any other electronic means of communication where personal details may be shared.

Responsibilities – School (Computing / PSHE leads)

- It is the responsibility of the school to ensure that a **member of staff is appointed to maintain the E-Safety Policy**, manage E-Safety training and keep abreast of local and national e-safety awareness campaigns. (The policy will be reviewed regularly and revised as appropriate to ensure that it is current and considers any emerging technologies.)
- School should audit the **filtering system** in place (currently part of the SwGfL services) regularly to ensure that inappropriate websites are blocked. Schools **should include e-safety in the curriculum** and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.
- All staff and pupils must read and sign our agreed Acceptable Use Policy (pupils discuss and sign Using the Internet Sensibly) (see appendices). The school will monitor the policy in practice, which will include Internet/e-mail usage and investigate and act on any possible incidents of misuse.
- The E-Safety Policy will be made available to all staff, governors and visitors.
- Sharing the school policy on e-safety and communicating potential risks will be an on-going responsibility of the school.

Responsibilities – Staff

All staff need to understand the potential risks involved in electronic communication and actively promote responsible uses of all appropriate technologies. Inappropriate uses could lead to disciplinary action and possibly even dismissal.

All staff should sign our Acceptable Use Policy (See appendix B) on appointment, thereby accepting that the school can monitor network and Internet use to help ensure staff and pupil safety.

All staff should **monitor the uses of technologies by the pupils** in their care and follow the recommended procedures for where any inappropriate or illegal ICT use is discovered. (See later in this document) Any allegation of inappropriate behaviour must be reported to senior management and investigated with great care - an innocent explanation may well exist.

E-mail, text messaging and IM(Instant Messaging) all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur, or communications can be misinterpreted. Apart from in exceptional or agreed circumstances, such as via the school blog site or other Managed Learning Environments, electronic communications between staff and pupils should be avoided.

Responsibilities – Pupils

The children in our school should benefit from the resources and activities available on the Internet, but should also be aware of the potential dangers. KS2 children should discuss and sign the 'Using the Internet Sensibly' document at the beginning of each year. **All teachers will use government and LA recommended resources to support e-safety activities. These highlight the need for adopting sensible and safe practices,**

including never divulging personal details, not accessing any undesirable material and reporting any concerns to a member of staff immediately.

Equal Opportunities

Every member of staff and every pupil in the school has the right to benefit from accessing any technologies that may benefit their working practices or learning.

Teaching and learning

E-Safety has a much higher profile and is specifically mentioned in the new Computing curriculum (2014) and will therefore be a more prominent aspect of the school curriculum.

The purpose of Internet use in school is to support and help raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions - it is a necessary tool for learning in today's society.

The Internet has widespread uses to support teaching and learning, including:

- 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;
- vocational, social and leisure use in libraries, clubs and at home;
- 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 LA and DCSF;
- access to learning wherever and whenever convenient.

Internet access should be planned to enrich and extend learning activities. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Unsupervised Internet access should be kept to a minimum and when pupils are working with greater levels of independence, such as in Year 6, staff should always be aware that the children are working responsibly.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Part of the school's role is to help pupils learn how to evaluate Internet information and to take care of their own safety and security. Pupils should be encouraged to reflect on and evaluate on-line materials and acknowledge the source of information used, respecting copyright when using Internet material in their own work. This process applies across all subjects.

E-Safety for pupils with additional needs

Where appropriate, the SENDCO will coordinate advice between ICT specialists and support staff in the case of individual pupils. This may take the form of child-focused strategies that would apply to a pupil with specific needs and would be made available to all staff involved in Internet use with that child.

Using the Internet

All staff must read and sign the appropriate Code of Conduct (See Appendix B) before using any school ICT resource. (This will usually be done on appointment)

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. As children progress through KS2 it may be that more independent access to the Internet is appropriate, but staff should always be aware that the Internet is being used responsibly. Children in KS2 will have the opportunity to discuss the 'Using the Internet Sensibly' document (see appendix C), before agreeing and signing a classroom copy.

Filtering

The school will maintain a filtering system to safeguard all users. Staff should also be aware however, that such systems are not foolproof and responsible use is still everyone's responsibility.

Searching

Internet searching, using technologies such as Yahoo and Google, has safe searching options and this should always be switched on. Image and video searching should be particularly closely monitored. When such resources are essential to the learning outcomes it is preferable that children select from resources previously downloaded by a member of staff. Where children are working with greater levels of independence they should be reminded of the need to search for things responsibly and understand what to do if anything undesirable is returned in the search results.

E-Mail

E-mail is an essential means of communication for both staff and pupils.

All

staff have access to a personal email account, whilst children, when appropriate, will use email to communicate under controlled conditions (e.g. just within the school domain). The school reserves the right to monitor email usage by all users, but will be much more active in monitoring pupil email accounts. Pupils may only use approved e-mail accounts and must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others, unless specifically approved by a member of staff. Under no circumstances should pupils arrange to meet anyone without specific permission. The forwarding of chain letters is not permitted.

Social Networking Sites (e.g. Facebook, Bebo, MySpace)

While social networking sites often provide a valuable tool for assisting communications between groups of friends or those with shared interests, they provide a risk to young people if used inappropriately.

The school will block/filter access to social networking sites via the school network and will teach children the dangers of publishing personal information, such as full name, address, phone number etc, and images on such sites. Although there should be no access to such sites from school, pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others.

It is possible that bullying can take place through social networking especially when a space has been setup without a password and school will work closely with pupils and parents to ensure this doesn't happen.

Blogging

The children have the opportunity to contribute to a selection of school blogs. We see this as a way of introducing many of them to some of the key ideas related to becoming sensible users of social media sites. The blogs can be used to:

- learn how to contribute to and interact responsibly with an online community
- share resources and notices
- share work and learning (providing a real authentic audience world-wide)
- provide up to date information on what is happening at our school.
- integrate multimedia of all descriptions (videos, photo stories, podcasts)
- receive feedback (we'd love to receive your comments and suggestions)
- post homework and extra learning experiences

As you can see the blog is an amazing tool that has huge potential to enhance children's learning.

Our key rules for blogging include:

- Only ever use your FIRST name on the blog
- Write using proper sentences, with as correct spelling as possible (no text speak – LOL!)
- Never put any PERSONAL DETAILS online - this includes phone numbers, addresses, personal email addresses or family information
- Only write positive comments or replies

All of the blogs are moderated by school staff to add an additional layer of protection to the children in school.

Video conferencing

Videoconferencing provides an exciting means of communicating between two or more locations. Although it is not an everyday occurrence, the following issues need to be considered.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information should not be put on the school Website.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
- Pupils should always ask permission and be supervised before making or answering a videoconference call.
- Parents and guardians should agree for their children to take part in videoconferences.
- Any video conferencing should be a planned experience that contributes to the development of our staff or pupils.

E-SSafety in the Classroom

Each class teacher will ensure that their children discuss some of the relevant issues and will use the pupil materials on the 'Think You Know' website for support. KS1 will use the 'Lee and Kim' and 'Hector' series of animations and KS2 will use the games and activities within the 8-10 age section. This could be done as part of normal curriculum work (e.g. as part of the e-mail unit in year 3), during PSHE sessions or at other times. Year 5 and 6 could watch the short 'Jigsaw' film, which illustrates the dangers of sharing personal information over the Internet. (See Appendix A). E- safety will also feature at assembly times during the year.

Electronic Publishing

The school website is our blog site. It provides an important insight into the life and philosophies of the school. It can be hugely motivating for children to have work published on blogs but the following should be observed.

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information must not be published (Staff photos and surnames are published on the school website to allow parents to put faces to names.) The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

Responding to an incident/concern/complaint

Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

What are the risks?

- | | |
|-------------------------------------|------------------------------------|
| - Receiving inappropriate content | - Publishing inappropriate content |
| - Predation and grooming | - Online gambling |
| - Requests for personal information | - Misuse of computer systems |
| - Viewing 'incitement' sites | - Publishing personal information |
| - Bullying and threats | - Hacking and security breaches |
| - Identity theft | - Corruption or misuse of data |

Depending on the nature of any issues that arise, the following processes should be used as guidance.

- If the issue has child protection implications, the designated school child protection coordinator should be contacted first. They will then manage the process in line with the school's child protection policy.
- If the issue relates to a teacher instigating some kind of undesirable behaviour the Head teacher and Computing subject leader should be contacted first. They will then manage the concern and involve other staff or agencies as necessary.
- Less serious issues should be discussed with either class teachers or the Head teacher and an appropriate course of action decided.

When deemed appropriate, the following options might follow a concern/complaint.

- Discussions with children/adults involved
- Contacting parents
- Counselling
- Discussions with police/Legal action
- Storage of computer equipment as evidence
- Further risk assessments and changes to procedures

Managing Information and data protection

ICT security is a complex matter and it is the responsibility of the Computing subject team, in conjunction with the Head teacher and Governors to maintain safe and secure working systems.

The Network Manager will be primarily responsible for ensuring the curriculum ICT infrastructure is up to date and secure (including servers, virus protection and wireless networks). The school office systems are maintained by the office manager.

Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive. Portable media (USB memory sticks) should be scanned regularly, especially when transferring data between computers.

Users must take responsibility for their network use.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

Files held on the school's network will be regularly checked.

The network manager will review system capacity regularly.

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

Emerging technologies

Many emerging communications technologies offer the potential to develop exciting teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. School has a responsibility to keep up to date with new technologies to maximise their use for education benefit.

This policy is written within the legal framework provided by the following Acts:

Racial and Religious Hatred Act 2006

Sexual Offences Act 2003

Communications Act 2003 (section 127)

Data Protection Act 1998

The Computer Misuse Act 1990 (sections 1 – 3)

Malicious Communications Act 1988 (section 1)

Copyright, Design and Patents Act 1988

Public Order Act 1986 (sections 17 – 29)

Protection of Children Act 1978 (Section 1)

Obscene Publications Act 1959 and 1964

Protection from Harassment Act 1997

Regulation of Investigatory Powers Act 2000

Appendix A – E Safety in the Classroom

Each class teacher will ensure that their children discuss some of the relevant issues and will use the pupil materials on the 'Think You Know' website for support.

KS1 will use the 'Hector' series of animations (in the 5-7 section) and KS2 will use the games and activities within the 8-10 age section.



This could be done as part of normal curriculum work (e.g. as part of the e-mail unit in year 3), during PSHE sessions or at other times. Year 5 and 6 could watch the short 'Jigsaw' film, which illustrates the dangers of sharing personal information over the Internet.

Key Stage 1

The following materials are available for use in the classroom. They can be accessed via the 'Think You Know' website (www.thinkuknow.co.uk).

Supporting documents (colouring pages (under the 'goodies' link) and some interactive jigsaw puzzles) are available on the website and some lesson plans.



Lee and Kim – These resources are aimed at younger children and introduce concepts such as keeping personal information private and playing sensibly online.

Hector – Cartoon 1 – Details, Details (Some personal details should not be shared online)

Hector – Cartoon 2 – Welcome to the Carnival (stranger danger, not everyone you meet is automatically trustworthy)



Hector – Cartoon 3 – It's a Serious Game (How can we know if a person can be trusted?)

Hector – Cartoon 4 – The Info Gang (Understanding our emotions)

Hector – Cartoon 5 – Heroes (Check with an adult before giving out personal details online)

Key Stage 2

The following interactive materials (games) are available on the 'Think You Know' website (www.thinkuknow.co.uk)

Most of these are short activities, that would support any incidents that occur during a school year, but some aspect of online safety should be included in every KS2 class at some stage during the year.

	Background Info and Tips
	Arcade style game – identifying 'spam' emails
	Which messages are safe to receive via Bluetooth
	What personal information should you share about yourself online.
	Simulated 'Chat' - reinforcing messages about sharing personal information
	Blockbuster style game, using e-safety related vocabulary
	Recognising safe and unsafe online activities/ideas
	Email simulation – identifying safe/unsafe content
	Identifying safe/unsafe ideas
	Simple 'What If' scenarios
	E-Safety Quiz
	Simulation – related to children's rights

Appendix B

Minchinhampton Primary Academy Acceptable Use of Digital Technologies: Staff

This document covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- It is advisable to use the school email system for any school business and where this is not used, I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not browse, download or send material that could be considered offensive to colleagues and will report any potentially dangerous/risky incidents.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will take every precaution to ensure that when I connect any electronic equipment (e.g. USB memory stick) to the school computers/network it is either scanned or if it is a laptop, has up to date virus software.
- Images of pupils will only be used in accordance with our E-Safety policy and as such if images are taken at school or on a trip on a personal device such as phone or tablet they will immediately be downloaded onto the school's secure system and then deleted from the device.
- Staff should inform the school if they object to their image being used for school purposes. (i.e. in such locations as the school website.)
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to do not compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will ensure I am aware of digital safety-guarding issues so they are

appropriately embedded in my classroom practice.

- I will only use LA systems in accordance with any corporate policies.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action and possibly even dismissal.

User Signature

I agree to abide by the school's most recent e-safety and acceptable use policies.

Signature Date

Full Name(printed)

Job title



USING THE INTERNET SAFELY

I agree to follow these rules when using the Internet in school

- 1. I will mainly use the Internet to help with my school work.**
- 2. I will only contact other Internet users with the permission of my teacher.**
- 3. I will never tell anyone any personal details about myself or other people (e.g. age, phone number, address, etc)**
- 4. I will only use links on the school website, or those provided by my teacher.**
- 5. I will only use a search engine with the permission of my teacher.**
- 6. I will not access any chat rooms or use messenger from a school computer or tablet.**
- 7. I will not download or upload any files or images without permission.**
- 8. If I am upset by anything I discover while using the Internet I will tell a teacher immediately.**
- 9. I agree to be a responsible user of the Internet and use it to help me develop my understanding and learn new things.**

Signed:

Date:

.....

.....

September 20__.

Dear Parents,

We often photograph our pupils learning in school. The photographs are an invaluable tool for celebrating and recording achievement. We will also sometimes put the same photographs onto the school blogsite as a way of celebrating their achievements to a wider audience. Sometimes photographs will end up being used for promotional purposes such as in the prospectus or on a leaflet.

Please let the school office know, in writing, immediately if you DO NOT AGREE to your child's photographs being used. If we do not receive written notification, your child's photograph may be used. Before declining to give your permission, please do consider how complicated it is for us on an organisational level to filter some pupils out of photographs. Also know that at no point is a child's photograph displayed with their full name. That said, there are sometimes very real personal reasons for wanting to keep a child's photograph out of the public arena.

Many thanks.

[Mr Moss](#)

Mr N Moss
Head teacher