St. Mary's CE (A) Primary School

E-Safety Policy

Policy written: November 2012 by Jane Hughes

Policy adopted by the Full Governing Body – Autumn Term 2012

Review of the policy will take place every two years or sooner if necessary.

Next review due: Autumn Term 2014

Signed:______________________________ **Dated:**______________
Jane Hughes – Headteacher

Signed:______________________________ **Dated:**______________
Sally-Ann Shotton – Chair of Governors

The School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

Why we need an e-safety policy

The Internet and communications technology are increasingly becoming a part of everyday life both in and out of school. The benefits of using these are immeasurable; they include discovering, connecting, creating and sharing. However, it is essential that young people and those responsible for them are aware of the issues surrounding safety when using these tools. We must protect our students while they operate within the school but it is essential to educate them for their use of technology outside of the school. We must empower children and young people to protect themselves in both the real and the virtual world.

The school's e-safety policy relates to use of the internet, digital communication technologies such as email and mobile phones.

The school's e-safety policy will operate in conjunction with other policies including Pupil Behaviour, Anti - Bullying, Data Protection and Safeguarding Children.

Assessing the school's level of development in e-safety

The school uses the WMNET e-safety framework to assess and benchmark its adoption of good e-safety practice across all e-learning activities.

The table below indicates the position the school is at:
(the levels relate to those identified in the WMNet e-safety framework)

Area of review	**School Level**
Acceptable Use Policy	1
Designated member of staff	1
Monitoring	1
School improvement planning	1
Teaching and curriculum	1
e-safety resources	1

Beyond school	1
Parents	1
Staff information literacy	1
Pupil information literacy	1

In order to be able to balance the huge educational benefits of Internet and electronic communications technologies with the potential risks, we need to first understand what these risks are.

Potential risks
Content
Children need to be protected from viewing and/or downloading adult material, violence, racist/hate sites, illegal drugs, software piracy.
Children need to understand that content found on the Internet may be inaccurate – as anyone can publish anything they wish on the Internet.
Children need to be made aware of the potential long term effects of any inappropriate content that they upload themselves, such as photographs, too much personal information or nasty comments about others.
In addition, children need to understand about inappropriate use of Internet content with respect to copyright issues.

Commerce
Children need to be protected from and educated about issues surrounding commercial marketing such as spam, phishing, pharming and the potential blur between content and advertising.

Communication
Children need to be made aware of and protected from the adverse issues concerning digital communication (i.e. you can never be 100% sure that you know who you are communicating with!). Safe use/potential dangers of email use, instant messaging, chat rooms, social networking sites etc need to be explored and made clear to pupils. The dangers of using digital imaging devices such as cameras and webcams to display images should be underlined.

Contact
There are people who will go to an immense amount of trouble in order to gain access to children in order to do them harm. The dangers of contact with persons unknown must be made clear.

Culture
The way that some children use the Internet can lead to depersonalisation (forgetting that in the virtual world, there is a real person) and this can lead to cyber bullying, which can become far more extreme and wide-ranging than 'face to face' bullying (Although we recognise that all bullying is completely unacceptable and needs to be dealt with as quickly and effectively as possible)

All members of a school community need to know about these dangers, how to avoid them and what to do if they feel threatened.

What do we do to prevent these potential dangers?

Internet safety co-ordinator
Becta recommends that each school has an Internet safety officer (this should be a member of the SMT), who will lead on establishing and maintaining a safe ICT learning environment in the school through the following:

Education

Ensure there is an Internet safety education programme in place for the whole school community. (Internet safety is a whole school responsibility, and many problems will occur out of school hours). For example:

- We need to educate children and young people about the benefits and risks of using new technologies both in and away from school. Pupils could, for example, take part in the Think U Know project. Children should be taught to seek help if they experience problems.
- Teachers and teaching assistants, support staff and governors need to be made aware of e-safety issues, and what to do in case of any problems.
- Parents have a key role to play in promoting safe Internet use and it would be in a school's interest to inform parents of possible risks and how to combat these.

Acceptable Use Policies

There should be appropriate AUPs for staff and for pupils (plus anyone else who regularly accesses school computers), which identify both rights and responsibilities. Pupil AUPs should be countersigned by parents. (Exemplar AUPs are available from http://www.wmnet.org.uk/wmnet/custom/files_uploaded/uploaded_resources/1698/AUP_Apr08.doc

The rules for safe and responsible Internet use will be displayed near the computers in Class 2 and Class 1.

Technological safeguards

There are many technological tools which are used in schools to keep children safe- all Staffordshire primary schools, use a Becta-accredited ISP, providing a firewall and virus protection, filtering and content control.

Pupil access

No primary school pupils should have unsupervised access to the Internet

Digital literacy

Pupils need to be taught to become discerning users of the Internet, understanding when and how to check the reliability and validity of a source and how to use the information effectively and honestly. Copyright issues need to be explained to the pupils and best practice modelled by staff.

Staff will not store photographs of pupils on their home computers or mobile phones.

Mobile phones

Pupils are not permitted to have mobile phones in school. If they need their mobile phone after school it may be safely stored in the school office during the school day. Staff are not permitted to keep their mobile phones switched on during the school day, however may access their phone, which is not stored in classrooms at break times.

Review own practice regularly

The school uses the WMNET e-safety Pledge in conjunction with the BECTA Self-Review Framework to identify practical steps to improve their e-safety provision and procedures.

What do we do if there is a problem?

Children must be made aware that they should report any incident that upsets or worries them, whether it be on the Internet, by mobile phone, email or text etc. We want to develop a culture where all such incidents are brought into the open.

It must be made clear to pupils who to contact if they are worried/upset by anything they see on the Internet/email etc. This would normally be their class teacher but could be the Internet safety co-ordinator. The school will adopt the 'Hector Protector' tool so that any evidence can be preserved.

Incident log

The school will maintain an incident log of all e-safety incidents

Minor incidents

If it is a 'minor' incident then it should be dealt with as per school procedure and documented so that there is a record of it should the problem escalate
Minor incidents, as defined in the Becta e-safety document ('Developing whole-school policies to support effective practice') are (for example) plagiarism; breaking copyright; downloading materials in breach of the school's AUP; using someone else's usernames and passwords; using own technologies e.g. mobile phone, against school rules, e.g. taking pictures of others on the camera, sending texts in lesson etc,

More serious incidents

A more serious inappropriate misuse (i.e. not illegal but not in keeping with school code of ethics) requires a strong disciplinary response from the school. The incident should be documented as above.
Examples of this, as defined by Becta, include soft pornography; hate material; drug or bomb making recipes; material others feel offensive- racist /sexist jokes, cartoons, low-level harassment; printing or transmitting offensive material; cheating in exams or coursework; hacking; gambling; intentional exhibiting of age-restricted materials to pupils under that age

Incidents involving adults

Any incident involving an adult as the perpetrator is a more serious matter and should be reported to the Internet safety coordinator who will document the incident and decide a course of disciplinary action which may involve the headteacher, external agencies, child protection etc. (Police need only be involved if a criminal offence has been committed) This should also lead to a review of Internet safety policies and procedures.
Should the incident attract any media attention, the school should contact the LA at once.

Criminal offences

If a criminal offence has been committed (by a pupil or member of staff), schools need to contact the police at the earliest possible opportunity. Evidence should not be deleted.
Criminal offences, as detailed in Becta e-safety documentation include involvement with illegal materials, particularly viewing, making, possessing or distributing indecent images of children. NB – if any such material is found, keep everyone away from the computer and touch nothing! Notify the police at once, but do not access/try to delete/copy the material in any way, but leave it exactly as you found it. Keep the computer turned on (monitor can be turned off.)
Serious 'cyberstalking', or serious harassment, including death threats or serious threats of harm, should be reported to the police.
In these cases, the school should contact the LA at once, who will arrange for legal advice.

Who has been involved in creating this policy, who is involved in its implementation and when it will be reviewed:

The policy has been written by all staff and agreed by Governors and parents, it is available for parents on the school's website and at new intake or induction meetings.

The headteacher oversees the implementation of this policy within her role and also the role of Child protection Co-ordinator.

E-Safety Co-ordinator:	Jane Newton
Governor Responsible:	Stephen Bayfield

Appendix A

- Acceptable Use Policies for Schools

Appendix A

WMnet E-safety

Acceptable Use Policies for Schools

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers, they may also arise through the use, for example, of games consoles and mobile phones.

There is an expectation that schools will have in place appropriate policies and strategies to promote the safety of learners in their care both when they are in the school and when they are elsewhere.

AUP Guidance notes for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not load photographs of myself onto the computer
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else

AUP Guidance notes for learners in KS2 and above

When I am using the computer or other technologies,
I want to feel safe all the time. .

I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- work in collaboration only with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult
- only use email which has been provided by school
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me

I know that once I post a message or an item on the internet then it is completely out of my control.

I know that anything I write or say or any website that I visit may be being viewed by a responsible adult
I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - pornography (including child pornography)
  - promoting discrimination of any kind
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
  - do anything which exposes children in my care to danger
  - any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law
- do anything which exposes children to danger

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety

- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff