E-Safety Policy

Lead Person/People	**L. Sutcliff**
Ratified by Governors	**December 2016**
Date for Review	**May 2018**
Signed – Governor	**Elizabeth Blake**
Signed – Headteacher	**Julia Sherlock**

Contents

1. Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid.

Current and emerging technologies used in the Academy and, more importantly in many cases, used outside of the Academy by children include:

The internet;
e-mail;
Instant messaging (www.msn.com) using simple web cams;
Blogs (an on-line interactive diary);
Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player);
Social networking sites (www.facebook.com);
Video broadcasting sites (www.youtube.com);
Chat Rooms (www.teenchat.com);
Gaming Sites (www.neopets.com);
Music download sites (www.limewire.com);
Mobile phones with camera and video functionality;
Smart phones with e-mail, web functionality and cut down 'Office' applications.

E-safety is included in the new National Curriculum for computing. One of its aims is to ensure that all pupils:

- **are responsible, competent, confident and creative users of information and communication technology.**

Additionally within the subject content for Key Stage 1, it states that pupils should be taught to:

- **use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.**

And within Key Stage 2 that pupils should be taught to:

- **use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.**

2. Policies and Procedures

The Academy's e-safety policy will operate in conjunction with other policies including: Behaviour, Anti-Bullying, Teaching and Learning and Data Protection. Our e-Safety Policy has been written building on BECTA government guidance. The e-Safety Policy and its implementation will be reviewed annually and where

necessary in cases of reported misconduct or risks.
All Academy staff and pupils are to sign an Acceptable Use Policy (AUP) detailing the ways that staff, pupils and all network users should use our ICT facilities. It also reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. The AUP is displayed in all classrooms and on laptop trolleys.

E-safety will form a key part of the Computing/PSHE/SEAL Curriculum. Children will be made aware of the dangers and risks of using the Internet and mobile technologies throughout the Academy year. This will include during anti-bullying week, e-safety awareness week and an integral part of Computing lessons.

3. Internet Access

The Internet is an essential element of education, business and social interaction. The Academy has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of our curriculum and a necessary tool for staff and pupils.

The Academy Internet access will be designed expressly for pupil use and will use appropriate filtering system.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will not use the internet without having permission from a member of staff.

Pupils will not use social networking sites in the Academy and will be educated about their safe usage in their own time.

Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.

Pupils are forbidden from downloading games or other programs from the Internet.

The ICT technician will carry out downloading programs from the Internet.

Public chat-rooms and instant messaging are not allowed and are blocked using the school's Internet filter (currently Openhive).

Access to peer-to-peer networks is forbidden in the Academy.

Pupils will be educated in 'Information Literacy' and taught how to evaluate the Internet content that they have located. Pupils will be taught the importance of crosschecking information before accepting its accuracy.

The Academy will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.

Pupils will be taught how to report unpleasant Internet content.

4. E-mail

When available, pupils may only use approved Academy e-mail accounts on the Academy network. Pupils are not permitted to use their own personal email accounts on Academy equipment.

Pupils must immediately tell a teacher if they receive an offensive e-mail.

In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.

Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.

Staff should never use personal e-mail addresses to communicate with pupils. The ICT technician will provide an official school e-mail address.

5. Virtual Learning Environment

The VLE (currently Moodle, although the Academy is currently looking into alternatives) is provided for use of the Academy staff and pupils only. At present access by any other party is strictly prohibited.

Pupils should never reveal his/her password to anyone or attempt to access the service using another pupil's login details. Pupils should inform the ICT technician if they feel their password has been compromised.

All staff and pupils possess a username and password as a level of security. The correct levels of privilege are applied to the correct users.

Activity on the Learning Platform will be monitored to ensure that the content posted by users is valid and does not infringe the intellectual property rights of others.

6. Published Content and the Academy Web site

Staff or pupil's personal contact information will not be published. The contact details given online should be the Academy office.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Permission from parents or carers will be obtained before photographs of pupils are published on the Academy web site.

Work can only be published with the permission of the pupil and parents.

Pupil image file names will not refer to the pupil by name.

Pupil image files should be securely stored on the Academy network.

7. Video Conferencing and Webcam Use

When available, video conferencing and webcam use will be appropriately supervised.

Pupils will be taught the dangers of using webcams outside of the Academy.

8. Portable Devices

Mobile phones are not to be used in the Academy; those children who walk home alone should leave them at the Academy office at the beginning of each day. The sending of abusive or inappropriate text messages is forbidden.

Staff should be aware that technologies such as Ultra Portable Laptops and mobile phones may access the Internet by bypassing filtering systems and present a new route to undesirable material and communications.

Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the Academy.

Pupils are taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

9. Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

Technologies such as mobile phones with wireless Internet access can bypass the Academy filtering systems and present a new route to undesirable material and communications.

Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access, which may not include filtering. These may not be used in the Academy unless supervised by staff and when used for specific purposes, e.g lunchtime clubs.

10. Protecting Personal Data

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

11. Roles and Responsibilities

The name of our Computing/e-Safety Coordinator/s and Computing/e-safety Governor is available from the school office.

Support will be provided by the IT technician. Our Computing Coordinator ensures they keep up to date with e-Safety issues and guidance; keeps the senior management and Governors updated as necessary; ensures that any e-safety concerns are reported in the first instance to the headteacher who will investigate the concern and take the appropriate action.

Our Governors have an understanding of e-Safety issues and strategies at the Academy, and are aware of local and national guidance on e-safety and are updated at least annually on policy developments.

Our staff have e-safety responsibilities: to be familiar with the policy and to adhere to its' procedures and must be familiar with the Academy's Policy in regard to:

Safe use of e-mail;

Safe use of internet;

Safe use of the school network, equipment and data;

Safe use of digital images and digital technologies, such as mobile phones and digital cameras;

Publication of pupil information/photographs and use of the web site;

E-Bullying / Cyber bullying procedures;

Their role in providing e-safety education for pupils;

Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential;

Staff will always use a child friendly, safe search engine when accessing the Internet with pupils. (e.g. Google Safe Search – default settings).

Academy staff will be reminded/updated about e-safety matters at least once a year, and receive training from a CEOP (Child Exploitation and Online Protection) instructor.

12. Managing Internet Access and Other Technologies

Information system security

Academy IT systems capacity and security will be reviewed regularly.

All staff and pupils possess individual logons and passwords to the Academy network with appropriate access rights and privileges.

Virus protection will be installed on all Academy computers and updated regularly in light of new viruses and Trojan horses that weaken the Academy's security.

Staff must ask permission from the Computing Coordinator / IT Technician before installing software on any Academy machines, which should normally be installed by the Network Manager.

Managing filtering

If staff or pupils discover an unsuitable web site, it must be reported to the Computing Coordinator and/or IT technician, the web site can be closed but the computer should not be shut down to allow further investigation.

The IT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Assessing risks

The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of internet access.

The Academy will give responsibility to the IT technician to monitor the use of Internet, email and messaging services.

The Academy should audit IT 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 the Computing / e-Safety Coordinator.

Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures (the designated person should be informed and a cause for concern form completed in line with the Academy's policy).

Pupils and parents will be informed of the possible consequences for pupils misusing the Internet.

Pupils and parents will be informed of the complaints procedure.

Discussions will be held with the police Neighbourhood Schools Officer to establish procedures for handling potentially illegal issues.

Enlisting parents' support

Parents' attention will be drawn to the Academy e-Safety Policy in newsletters, the Academy brochure and on the Academy web site.

Parents will be given a copy of the Acceptable Use Policy that their child has signed. They will be encouraged and supported to monitor their children's use of technology at home.

The Academy will provide regular e-safety updates for parents in the form of letters and where appropriate practical sessions.

Annex 1 – E-Safety Glossary

The definitions used in the E-Safety Policy are:

Acceptable Use Policy: A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

Becta: The Government's lead partner in the strategic development and delivery of its e-strategy from 1998-2011.

Chat-room: An area on the Internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the Internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant messaging (IM): A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Peer-to-peer (P2P): A peer-to-peer network allows other users to directly access files and folders on each other's computer. File sharing networks such as 'Lime Wire' creates weaknesses in networks security by allowing outside users access to the schools resources.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses: A virus, which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Video Conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus: A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard

drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A webcam is a camera connected to a computer that is connected to the Internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

When using the internet

S 	I will only use the internet when I have an adult's permission.
A 	I will only click on icons and links when I know they are safe.
F	I will only send friendly and polite messages. I will not give away any personal information.
E	If I see something I don't like on a screen I will close it down and tell an adult immediately.
	During wet play I will ONLY go on websites agreed as a class.

THINK BEFORE YOU CLICK

I understand how to be safe when using the internet.

Name: **Class:**

Annex 3 – Rules of Acceptable Use of the Computers

The Academy has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret. I will let the ICT Technician know if I need to change my password.
- I will not access other people's files.
- I will only use the computers for schoolwork and homework.
- Pupils should not download and use material or copy and paste content which is copyright. (Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the Internet).
- I will not bring in memory sticks or disks from outside the Academy unless I have been given permission.
- I will ask permission from a member of staff before using the Internet.
- I will only e-mail people I know or my teacher has approved using the Academy network. I will only use my Academy e-mail account.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.
- I understand that the Academy may check my computer files and may monitor the internet sites I visit

All children must sign the AUP before using an Academy computer
Book of signatures to be hung next to computers.