E-Safety Policy

Established: February 2017
To be reviewed: February 2018

Contents:

Key Vocabulary used in this document:

- Pharming (pronounced farming) is a hacker's attack aiming to redirect a website's traffic to another, bogus website.
- Phishing is the attempt to fraudulently acquire sensitive information (e.g., passwords, account numbers, or financial information) by masquerading as a trustworthy person or business in a seemingly official communication.
- Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers.
- Mobile blogging (moblogging) is a form of blogging in which the user publishes blog entries directly to the web from a mobile phone.

Keeping the Millom School community safe

1. **Rationale** "For young people ICT is not a novelty but the way they engage with their world - 21st century culture"

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 use of New Technologies can introduce a number of risks which can be categorised as:

- Content - sexual, racist, violent, unreliable i.e. safety of the mind of the child
- Commerce - scams, phishing and pharming, bluejacking, downloads which steal information - students and parents
- Contact - via interactive technologies – Instant Messaging, social media, multiplayer games
- Culture - bullying, camera phones, blogging, moblogging, social networking

Millom School has a duty of care, both inside and outside, to protect students from these risks. This policy aims to raise awareness of the risks involved when embracing new technologies for Internet Safety, Internet Security, Media Literacy and communications.

The school's e-safety policy will operate in conjunction with a range of other school policies including those for Student Behaviour, Bullying, Curriculum/Teaching & learning, Data Protection and Security.

The E safety policy is underpinned by the five intended outcomes of 'Every Child Matters', in respect of Staying Safe, Being healthy, Positive Contributions, achieving Economic Well Being and Enjoyment.

The e-Safety Policy

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

- Responsible ICT use by all staff and students; encouraged by the clarity of the policies and the rigorous approach to training and education to ensure consistency in its application across the school and through school-home links.
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use. This entails clear operational systems and quality assurance procedures to ensure the effectiveness of the policies.

- Safe and secure broadband from the Cumbria & Lancashire Broadband Consortium (CLEO) including the effective management of filtering.
- National Education Network standards and specifications.

2. School e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The Assistant Head: Student Support will be the E-safety coordinator.
- The E-Safety Policy has been written by the students and adults of the school. Building on the Cumbria County Council and government E-Safety Policy and guidance. It has been agreed by senior management and approved by governors.

2.2 Teaching and learning

2.2.1 Why Internet use is important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students, particularly in development of research and other transferable skills for promoting independent learning.

2.2.3 Internet use will enhance learning

- The school Internet access will be designed specifically for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear guidance regarding internet use. Each year group will be provided with guidance and training through the ICT/Computer Science curriculum, whole school awareness days/weeks, Personal Development lessons and Assemblies.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Teachers will, where appropriate, screen and identify web based sources that promote accessibility and inclusion in the learning process.

2.2.4 Students will be taught how to evaluate Internet content

Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law. Unauthorised audio (mp3) and video files will be removed from the network.

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

If staff or students discover unsuitable sites the URL (or website address) and the content must be reported to the Network Manager. Such sites will be added to the filtered websites database.

2.3 Managing Internet Access

2.3.1 Information system security

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

2.3.2 E-mail

- Students are recommended to only use approved e-mail accounts on the school system. A school based @millom.cumbria.sch.uk address is used to discourage the use of hotmail, msn email accounts, for example.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and and ensure the school disclaimer message is displayed at the footer of the email.
- The forwarding of chain letters is not permitted.
- The school has a sanction policy applied to students who infringe their internet access privileges. Students who continually abuse their email or violate their Internet access rules privilege will have their account barred for two weeks from the date of incident and a letter sent home.
- Emails will be scanned when sent for keyword content. Email content which is unsuitable will not be sent and a copy of the offending email copied to the systems manager for follow up with the Assistant Headteacher for Student Support.

2.3.3 Published content and the school web site

- The contact details on the website are the school address, e-mail and telephone number. Staff or students personal information will not be published.
- The headteacher or nominee (PJ Baggaley) will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Access to editing content on the School website is restricted to:
    - Network Manager
    - ICT network technician
    - Head of Computer Science

2.3.4 Publishing student's images and work

- Photographs that include students will be selected carefully and will be only be displayed in cases where relevant permission has been granted or the students are not clearly identifiable.
- Students' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site. This will be gathered through the Millom School AUP (Acceptable Use Policy) obtained from parents or carers at the start of an academic year.
- Work can only be published with the permission of the student and parents.

2.3.5 Social networking and personal publishing

- School will block and / or filter access to social networking sites, unless the sites are approved by the school for learning purposes.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. They will be taught how to make secure passwords – following guidance in the schools password policy.

2.3.6 Managing filtering

- The school will work in partnership with the LA, DfE and the Internet Service Provider (CLEO) to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the Assistant head: Student Support or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing

- Students should ask permission from the supervising teacher before making or answering a videoconference call. Calls should only be initiated by staff.
- Videoconferencing will be appropriately supervised for the students' age.

2.3.8 Managing emerging technologies

- 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, unless directed to by the class teacher for learning purposes. The sending of abusive or inappropriate text messages is forbidden. The recording of video using a mobile phone during lessons is forbidden unless directed by the classroom teacher.

- Students and staff can use mobile devices (including phones) outside of lesson time as long as it is in adherence with the Millom School Acceptable Use Policy for mobile devices.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Only authorised personnel will be able to edit personal details stored in the Management Information System.
- Whilst it is not possible to prevent loss of data due to mislaying a portable memory device, reminders will be placed around the school. Staff will be informed about the consequences of lost data including data files, images and lesson resources.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read the 'ICT Code of Conduct' before using any school ICT resource. This is published in the School Handbook on the VLE.
- Students and Staff will only be granted access to the Schools ICT network (including Internet access) if they have read, agreed and signed the School's Acceptable Use Policy.
- The school will maintain a current record of all staff and students who are denied access to school ICT systems.

2.4.2 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. The school can not accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.
- The school will ensure that antivirus databases and firewalls are kept up to date. Files copied on the network from CD ROMs, memory stick (or other portable storage device such as an mp3 player), DVD or laptop will be scanned for harmful content.
- Regular checks are undertaken to ensure illegal content is not stored on the network.

2.4.3 Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.

- There may be circumstances where police involvement is necessary, in which case the school will establish the legal position early and help to develop a strategy to resolve the issue/s.
- Any complaint made about staff misuse of the Internet must be referred to the Headteacher.

Consequences for eSafety Infringement:

- Depending upon the severity of the first offence the Head of ICT or Assistant Headteacher: Student Support will discuss the offence and issue a warning to the student. The offence will be logged on the SIMS behaviour management system by the Student Support Team Admin Assistant.
- For serious offences the evidence will be collated and a letter sent home describing the offence committed with associated evidence. This will be accompanied by a telephone call home. Students will have their Internet Access terminated for a period of time. This may also prevent the student from accessing files held on the system including examination coursework. All information will be logged on the SIMS behaviour management system.
- Where E-safety has been breached by a student the Assistant Headteacher: Student Support will follow-up and apply the school sanction policy where and when appropriate.

2.4.4 Classroom Internet Control

- The school will ensure that ICT staff are trained to use AB Tutor to monitor student activity in the classroom, block Internet Access for the whole class or individuals or limit activities to set URL's (website addresses)
- AB Tutor will be available to use in all ICT classrooms [to check that this is the case]. Outside of these areas staff can contact ICT Support to make their requests.

2.4.5 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to E-safety.
- The school will provide a guest log in username and password for when guests arrive wishing to use ICT facilities. Access to shared drives will only be made if necessary by the Network Manager.

3.2 Staff and the E-Safety policy

- All staff will be given a copy of the school E-Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff and students will be reminded not to leave work stations logged on in areas where others can gain access e.g. empty classrooms, ICT rooms.
- Students and staff (unless permitted) will not be able to download and install executable files from the internet (or elsewhere). Unauthorised files discovered on the network will be recorded, logged and deleted by the Network manager.
- Students found to be accessing banned websites by Proxy (i.e. using a website which allows you to type in the address of a banned website to gain access to it) will be interviewed by the Assistant Headteacher: Student Support and/or the Network Manager. For serious abuse cases, a letter will be sent home and the content of the website accessed listed. The website used by the student will be added to the filtered list and passed to the Local Education Authority.

3.3 Enlisting parents' support

- Parents' attention will be drawn to the school E-Safety Policy in newsletters, the school prospectus and on the school Website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Parents interested in child E-Safety matters will be referred to organisations such as CEOP (Child Exploitation and Online protection.)
- Advice will be given to parents about filtering systems and responsible Internet use upon request.
- Training will be provided throughout the Year, which will be open to both current and potential parents of the school. The timetable schedule on the following pages, contains further details.

3.4 Training & guidance

- Students will be provided with core training through their ICT/ Computer Science curriculum, school assemblies and whole school focus days or weeks e.g. Safer Internet Day.
- There will be opportunities for staff training during the school year.

E-safety School Review

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that would contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Headteacher.

Has the school an e-Safety Policy that complies with Cumbria guidance?	**Y/N**
Date of latest update (at least annual):	
The school e-safety policy was agreed by governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both students and staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Have e-safety materials from CEOP and Becta been obtained?	**Y/N**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y/N**
Are all students aware of the School's e-Safety Rules?	**Y/N**
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Has an ICT security audit has been initiated by SLT?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. CLEO)?	**Y/N**
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	**Y/N**
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	**Y/N**