

E-Safety Policy and Acceptable Use Agreement

**Introduction**

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

 At St Mary’s Primary School, Mullymeskerwe understand the responsibility to educate our pupils in E-Safety (*Electronic Safety*) issues.

The Internet is an integral part of pupils’ lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety. Child Exploitation and Online Protection (*CEOP*) resources are a useful teaching tool for all Key Stages looking at Internet safety and can be usefully incorporated into PDMU or ICT lessons.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.



This CEOP link is available on all MySchool desktops and on school website.

**Key concerns with using the internet**

**Potential Contact**

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons. Children should be taught:

* That people are not always who they say they are.
* That “Stranger Danger” applies to the people they encounter through the Internet.
* That they should never give out personal details.
* That they should never meet alone anyone contacted via the Internet.
* That once they publish information it can be disseminated with ease and cannot be destroyed.

**Cyber Bullying**

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the schools overall anti-bullying policy and pastoral services as well as the E-Safety policy.

Cyber Bullying can take many different forms and guises including:

* Email – nasty or abusive emails which may include viruses or inappropriate content. The CEOP link is available on all MySchool desktops.
* Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
* Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user’s profile.
* Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
* Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also

occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.

* Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person’s permission.

**Inappropriate Content**

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the

Internet.

Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual

content.

Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and

racism which would be restricted elsewhere.

Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities

which are harmful such as anorexia or bulimia.

Children should be taught: -

* That information on the Internet is not always accurate or true.
* To question the source of information.
* How to respond to unsuitable materials or requests and that they should tell a teacher/adult

immediately.

**Excessive Commercialism**

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

* Not to fill out forms with a lot of personal details.
* Not to use an adult’s credit card number to order online products.

**Roles and Responsibilities**

The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

The Principal/ICT Co-ordinator update all staff and Governors with regard to E-Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

**Teaching and Learning**

**Internet use:**

* The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.
* Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
* Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of

 staff, or an organisation such as Childline/CEOP.

* The school Internet access is filtered through the C2k managed service.
* Children are provided with technology in school and so they are not permitted to bring in their own devices to access the internet in school.
* No filtering service is 100% effective; therefore, all children’s use of the Internet is supervised by an adult.
* Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
* Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

**E-mail:**

* Pupils may only use C2k 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.
* The forwarding of chain mail is not permitted.
* Children are not always given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

**Social Networking:**

* The school C2k system will block access to social networking sites.
* Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
* Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
* Our pupils are asked to report any incidents of bullying to the school.
* School staff will not add children or parents as ‘friends’ if they use these sites.

**Managing Video-conferencing:**

* Where appropriate will be via the C2k network to ensure quality of service and security.
* Videoconferencing will be appropriately supervised.

**Publishing Pupils’ Images and Work**

* permission from parents or carers will be obtained before photographs of pupils are published on the school Website/Newsletter. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue.
* Parents/carers may withdraw permission, in writing, at any time.
* Parents will be reminded prior to any group performance that any photos/videos taken are not to be published in any public domain.
* Pupil’s work can only be published by outside agencies with the permission of the pupil and parents.

**Policy Decisions:**

**Authorising Internet access**

* These E-Safety rules will be displayed clearly in all rooms.
* Access to the Internet will be supervised.
* All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school’s E-Safety rules and within the constraints detailed in the school’s E-Safety policy.

**Password Security:**

Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.

* All pupils are provided with an individual login username and password.
* Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
* Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network systems.

**Handling E-Safety Complaints:**

* Complaints of Internet misuse will be dealt with by a School Principal.
* Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the E-Safety incident logbook.
* Any complaint about staff misuse must be referred to the Principal.
* Complaints of a child protection nature must be dealt with in accordance with school child protection

**Communicating the Policy:**

**Introducing the E-Safety Policy to pupils**

* E-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU, PATHs lessons/circle times/antibullying /Internet Safety Week.
* Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the **Thinkuknow website.**
* Pupils will be informed that network and Internet use will be monitored**.**
* There are various pupil resources available such as:

**Signposts to Safety** (primary and secondary versions)

Key Stage 2- 4

**KidSMART**

**Know IT All for Schools**

**ThinkUKnow**

**Childnet’s Sorted website**

.

**Monitoring and review:**

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Coordinator. This policy is the Governors’ responsibility and they will review its effectiveness regularly. They will do this by liaising with the ICT Co-ordinator and Designated Child Protection Co-ordinator.