E-Safety Policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communication Technology covers a wide range of resources including, web-based and mobile learning. It is also important to recognize the constant and fast placed evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, instant messaging and chat rooms
- Social media, including Facebook and Twitter
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning environments
- Blogs and Wikis
- Podcasting
- Video Conferencing
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not constantly policed. All users need to be aware of the range of risks associated with the use of these Internet technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Policy/Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices.

In City of Armagh High School, we understand the responsibility to educate our pupils in E- Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the classroom.

E-Safety is short for electronic safety.

It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

E-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world
- emphasises learning to understand and use new technologies in a positive way
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online
- is concerned with supporting pupils to develop safer online behaviours both in and out of school
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

The rapidly changing nature of the internet and new technologies means that E-Safety is an ever growing and changing area of interest and concern. The school's E-Safety policy reflects this by keeping abreast of the changes taking place. Our school has a duty of care to enable pupils to use on-line systems safely.

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.
- Pupils are not always given individual e-mail addresses. In some instances they may have access to a group e-mail address to communicate with other pupils 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 will be advised that when using social network spaces outside school they should never 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.
- School staff are requested not to add pupils or their parents (with the exception of work colleagues) as 'friends' if they use these sites.
- Parents and pupils should not request school staff as "friends".

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be approved by the teacher and will be closely monitored as potential sources of computer virus and inappropriate material.
- Pupils' mobile devices/ phones should be switched off whilst on school premises. Pupils failing to do so will be dealt with as per Positive Behaviour Policy.
- All staff should refrain, as far as possible, from using personal mobile devices/ phones during pupil contact time.
- Staff should not record images of pupils on their personal mobile devices/ phones.

Managing Video-conferencing:

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

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before images of pupils are published on the school website, displays, school newsletters or any publication which the school deems appropriate. 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.

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the internet is an essential skill for children as they grow up in the modern world. The internet is, however, an open communication channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key Concerns are:

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

Inappropriate Content

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 i.e. they should tell a teacher/adult immediately.

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 school's overall anti -bullying and pastoral care policies as well as the E-Safety policy.

Care should be taken when making use of social media for teaching and learning. Each of the social media technologies can offer much to schools and pupils but each brings its own unique issues and concerns. Each social media technology that is to be utilised should be risk assessed in the context of each school situation.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content
- 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.

Whilst cyber bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber bullying, the following may cover different elements of cyber bullying behaviour:

- Protection from Harassment (NI) Order 1997
- http://www.legislation.gov.uk/nisi/1997/1180
- Malicious Communications (NI) Order 1988
- http://www.legislation.gov.uk/nisi/1988/1849
- The Communications Act 2003
- http://www.legislation.gov.uk/ukpga/2003/21

It is important that pupils are encouraged to report incidents of cyber bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases. Should the incident occur outside school time, school will offer advice re: blocking number, reporting abuse etc. Should the cyber bullying impact on school life, the incidents will then be dealt with as per the school's Positive Behaviour and Anti Bullying Policies.

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.

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.

E-Safety – Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator in this school is Mrs K. Mulholland (Vice Principal & Pastoral Care Coordinator) who has been designated this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety, ICT and C2K co-ordinators to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The E-Safety, ICT and C2K co-ordinators have responsibility for leading and monitoring the implementation of E- safety throughout the school.

Senior Leadership and Governors are updated by the Principal/ E -Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use agreements for staff and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Home–School agreements, Positive Behaviour, Anti-bullying and P.D.

Teaching and Learning

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote it

- The school's internet access is filtered through the C2K managed service
- No filtering service is 100% effective, therefore, all pupils' use of the internet is supervised by an adult
- The school has a framework for teaching internet skills in ICT/ PD lessons
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating pupils about the online risks that they may encounter outside school is done informally

when opportunities arise and as part of the e-Safety curriculum

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
- 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 staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

E-Safety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas
- Ms J.Hughes, Designated Teacher for Child Protection is a CEOP Ambassador.

Communicating the School E-Safety Messages

Introducing the E- Safety Policy to Pupils

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-Safety policy will be introduced to the pupils at the start of each school year
- E-Safety posters will be prominently displayed
- Specific lessons/ assemblies will be delivered at relevant points throughout the school year e.g. Anti – bullying week, Internet Safety Week
- Through the use of workshops delivered by outside agencies e.g. PSNI, Love For Life.

Staff and the E- Safety Policy

- All staff will be given the school's E – Safety policy and its importance explained
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Policy Decisions:

Authorising Internet Access

- Pupil instruction in responsible and safe use should precede any internet use and all pupils must sign up to the school's Acceptable Use Agreement and abide by the school's E- Safety rules.
- Access to the school's internet will be supervised.
- All parents will be asked to sign the school's Acceptable Use Agreement for Pupils, giving their consent for their child to use the internet in school and abide by the school's E- Safety rules and within the constraints of the school's E- Safety Policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security

- Adult users are provided with an individual login user name and password which they must change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password
- Pupils are not permitted 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.

Handling E- Safety Complaints

- Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's ICT/ C2K or E-Safety Coordinator.
- Complaints and/or issues relating to E-Safety should be made to the E-Safety coordinator or the Principal.
- Any complaints about staff misuse must be reported to the Principal
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety coordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety coordinator. Depending on the seriousness of the offence; there may be an investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Users are made aware of sanctions relating to the misuse or misconduct through the school's Acceptable Use Agreement
- Pupils and parents will be informed of the complaints' procedure.

Monitoring and Reviewing the E-Safety Policy

This policy supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is monitored by the E- Safety co coordinator and is implemented by all school staff on a daily basis.

The policy is used to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Positive Behaviour, Health and Safety, Safe Guarding and Child Protection, and Anti-bullying.

It has been agreed by the Senior Leadership Team and staff and has been approved by the Board of Governors. The E-Safety Policy and its implementation will be reviewed annually by the E-Safety coordinator and the Designated Teacher for Child Protection.

Revised June 2016