
# ‘E-Safety’ Policy

*"All schools should have their own E-Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. E-Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills."*

**DENI E-Safety Guidance, Circular number 2013/25**

E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. The main areas of risk for the School can be categorised as the Content, Contract and Conduct of activity.

1. **Content**

   Access to illegal, harmful or inappropriate images or other content.
   Access to unsuitable video / internet games.
   An inability to evaluate the quality, accuracy and relevance of information on the Internet.

- **Contact**

  Inappropriate communication / contact with others, including strangers.
  The risk of being subject to grooming by those whom they may make contact with on the Internet.
  Cyber-bullying.
  Unauthorised access to / loss of / sharing of personal information.

- **Conduct**

  The potential for excessive use which may impact on the social and emotional development and learning of the young person.
  The sharing / distribution of personal images without an individual's consent or knowledge.

It is important that the E-Safety policy is used in conjunction with other school policies e.g. Child Protection and Acceptable Use. As with all other risks, it is impossible to eliminate risk completely. It is therefore essential, through good educational practice to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

*"21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity, they will need to learn to recognise and avoid these risks — to become 'Internet-wise' and ultimately good 'digital citizens'. Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy."*

**DENI E-Safety Guidance, Circular number 2013/25**

## Roles and Responsibilities

**ICT Coordinator**

The ICT Coordinator will:

- ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- deliver training and advice for staff.
- provide events, training and resources for educating pupils and parents E-Safety.
- liaise with C2K and school ICT technical staff.
- liaise with the EA and DENI on E-Safety developments.
- receive reports of E-Safety incidents and create a log of incidents to inform future E-Safety developments.
- work with Designated Child Protection staff to investigate abuse of social network sites by pupils.
- monitor and report to the Principal any risks to staff or pupils.

**Designated Child Protection Officer**

The Child Protection Officer (and their deputy) will be aware of e-safety issues and the potential for serious child protection issues to arise from:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate online contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

**Network Managers**

Network Managers and Technical Staff should regularly monitor that:

- C2K e-safety measures, as recommended by DENI, are working efficiently within the school.
- C2k / Fastnet operates with robust filtering and security software.
- monitoring reports of the use of C2k / Fastnet are available on request.
- the school infrastructure and individual workstations are protected by up to date virus software.
- the school meets required e-safety technical requirements that users may only access the networks and devices through a properly enforced password protection policy.

**Teaching and Support Staff**

The Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of E-Safety matters and of the current school policy and practices.
- they have read and understood the school's Acceptable Use Policy.
- they report any suspected misuse or problem to the ICT Coordinator.

- digital communications with students and staff (e.g. Email, Fronter, VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School's guidance.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- staff understand and follow the school E-Safety Policy and Acceptable Use Policy.
- they monitor ICT activity in lessons, extracurricular and other school activities.
- they are aware of e-safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- undertake all e-safety training as organised by the school.
- should report immediately to ICT Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

**Pupils**

Pupils are responsible for ensuring that they:

- use the school ICT systems in accordance with the Acceptable Use Policy.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- know and understand school policies on the use of mobile phone, digital cameras and hand-held devices.
- should also know and understand school rules on the taking/use of images and on cyber-bullying.
- understand the importance of adopting good e-safety practice when using digital technologies out of school.
- should report immediately to ICT Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

**Parents**

Parents and carers play a crucial role and will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- online communication with staff.
- their children's personal devices in the school.

## Current Practice

**E-Safety Education for Pupils**

E-Safety education for pupils will be provided in the following ways:

- a planned e-safety programme will be provided as part of ICT / PDMU and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources will be used as a teaching tool.
- pupils will be taught in all relevant lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- pupils will be helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

**Parents Training and Support**

Parents and carers have essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The School will seek to provide information and awareness to parents and carers through:

- a section of the school website will provide links to external sites such as CEOP.
- letters, newsletters, websites.
- updates and useful information shared through our social media sites.
- a designated E-Safety Parents' Event.

**Cyber-bullying**

Cyber Bullying can take many different forms and guises including:

- **Email** – nasty or abusive emails which may include viruses or inappropriate content.
- **Instant/Direct Messaging (IM/DM) 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. Use of group chat to intimidate or humiliate. 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.

- Incidents of cyber–bullying will be treated seriously and dealt with in accordance with the School Anti-Bullying Policy.

**Communication**

- The official school email service may be regarded as safe and secure. Staff should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Email communications with parents and/or pupils should be conducted through the following school email systems '@c2kni.net' Personal email addresses should not be used.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers - email, VLE and official school social media accounts - must be professional in tone and content. When emailing, staff should CC any communication to pupils to another member of staff.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**Social Networking**

- At present, the school endeavours to deny access to social networking sites to pupils during school hours.
- Teachers should be aware of the appropriate use of social networking in their private life - acceptable use; social media risks; checking of settings; data protection; reporting issues; legal risks.
- Teachers should adhere to the social networking / communication guidance provided by the school.
- Older students should be made aware of the appropriate and safe use of Social Networking
- Teachers and pupils should report any incidents of cyber-bullying to the school.

**Personal Devices**

- Pupils' mobile phones and personally-owned devices should not be brought into school.
- If a phone or device is brought to school it should be given to the class teacher and will be stored in a secure place.
- Pupils should be encouraged to protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and should only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, a senior member of staff should be informed and they should conceal their own mobile number (by inputting 141) for confidentiality purposes.

**Digital and Video Images**

- When using digital images, staff should inform and educate pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. Social Networking websites.
- The school gains parental / carer permission for use of digital photographs or video involving their child as part of the school data capture form when a child enrols.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those image.
- We will also ensure that when images are published that the pupils cannot be identified by the use of their names.
- Pupils must not take, use, share, publish or distribute images of other without their permission.
- The use of digital / video images plays an important part in learning activities and should be respected by staff and pupils.

## Security

**Teaching and Support Staff Passwords**

- Password security is essential for staff, particularly as they are able to access and use student data.
- Staff are expected to have secure passwords which are not shared with anyone.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.

**Student Passwords**

- Pupils' should be informed of the schools Acceptable Use Policy.
- Students are expected to keep their passwords secret and not to share with others, even their friends.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

**Digital Server Storage**

The school uses digital server storage for pupils and staff, the listed services have robust privacy policies and are committed to not sharing or misusing digitally stored information. When uploading to digital storage the website E-Safety principles will apply, e.g. no identification of pupils by full names. The privacy policies can be found for the following services:

- Apple iCloud: https://www.apple.com/uk/legal/privacy/en-ww/
- Google Drive: https://www.google.com/policies/privacy/
- Seesaw: https://web.seesaw.me/privacy

*Reviewed*
*R Goudy 2017*