CARRICKFERGUS GRAMMAR SCHOOL
E-SAFETY POLICY

Carrickfergus Grammar School policy on:	**E-SAFETY**
Date implemented:	September 2016
Review date / led by:	Sept 17, P Irwin (E-Safety Coordinator)
Consulted:	Governors, Parents, Pastoral Team
Allied School Policies: Child Protection, Anti Bullying, ICT Acceptable Use Guidance, Acceptable Use Mobile Phones	

1. Rationale

"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

It is the responsibility of the schools, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The School must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

This policy has been informed by DENI circular 2013/25 E-Safety Guidance and 2011/22 Internet Safety.

2. Scope of the Policy

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of the School. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure E-Safety of all involved, apply sanctions as appropriate and review procedures. In relation to E-Safety incidents that occur outside of school hours, the School will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of E-Safety incidents outside of the School, will be dealt with in accordance with School Policies.

3. Risk Assessment

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

The main areas of risk for the School can be categorised as the Content, Contact 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.

2. Contact

- Inappropriate communication / contact with others, including strangers eg. Sexting

- The risk of being subject to grooming by those whom they may make contract on the Internet.

- Cyber-bullying.

- Unauthorised access to / loss of / sharing of personal information.

3. Conduct

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The sharing / distribution of personal images without an individual's consent or knowledge.

Many of these risks reflect situations in the offline world and it is essential that this E-Safety policy is used in conjunction with other School policies e.g. Positive Behaviour, Child Protection, Anti-Bullying and Acceptable Use Mobile devices.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision 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.

4. Roles and Responsibilities

4.1 E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the Schools policies/documents.

The E-Safety 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.
- Liaise with C2K and school ICT technical staff
- Liaise with the EA and DENI on E-Safety developments
- Meet with Head of Pastoral Care when required to investigate e-safety issues
- Discuss current issues
- Monitor and report to senior staff any risks to staff of which the E-Safety coordinator is aware

4.2 E-Safety Officers / Designated Child Protection Officer / Deputy Designated Child Protection Officer

The Child Protection Officer (and their deputy) will be trained in e-safety issues and be aware of 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, including Sexting

- Potential or actual incidents of grooming

- Cyber-bullying

4.3 The Principal and Senior Leadership Team:

The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, but the day-to-day responsibility for e-safety will be delegated to the E-Safety Officer. The Principal and E-Safety Officer will be kept informed about e-safety incidents. The Principal will deal with any serious e-safety allegation being made against a member of staff. The Principal and SLT are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

4.4 Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

4.5 Network Managers – Paul McKittrick/Michael Blair

The Network Managers will monitor that C2K e-safety measures, as recommended by DENI, are working efficiently within the school.

- that C2k operates with robust filtering and security software

- that monitoring reports of the use of C2k are available on request

- that the school infrastructure and individual workstations are protected by up to date virus software.

- that the school meets required e-safety technical requirements that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed, the filtering policy is applied and that its implementation is not the sole responsibility of any single person, that they keep up to date with E-Safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

4.6 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 E-Safety policy and practices.

- They have read and understood the school's Staff Social Networking Policy along with Child Protection Procedures and the Staff Code of Conduct.

- They report any suspected misuse or problem to the E-Safety Coordinator.

- Digital communications with students (email / Virtual Learning Environment (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.

- Staff understand and follow the school E-Safety Policy and Staff Social Networking Policy.

- They monitor ICT activity in lessons, extracurricular and extended school activities.

- Undertake all e-safety training as organised by the school

4.7 Professional Development for Teaching and Support Staff

Training will be offered as follows:

- All new staff will receive e-safety training as part of their Induction Programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

- This e-safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

4.8.1 Pupils

Are responsible for ensuring that:

- They use the school ICT systems in accordance with the Pupil Acceptable Use Guidance, which they will be expected to sign before being given access to schools systems.

- They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.

- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- They know and understand school policies on the use of mobile phone, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

- Pupils are introduced to email and taught about the safety and ‘netiquette’ of using email both in school and at home

- They understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s e-safety Policy covers their actions out of school, if related to their membership of the school. This is developed through Assemblies, PSNI visits and education in Personal Development classes

4.8.2 E-Safety Education for Pupils

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

- A planned e-safety programme will be provided as part of PD / LLW / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

- 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 and to respect Copyright when using material accessed on the Internet.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- Pupils will be made aware of the importance of filtering systems. They will also be warned of the consequences of attempting to subvert the filtering system.

- Assemblies will be delivered explaining the issues surrounding E-Safety.

4.8.3 Parents / Carers

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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.

5. Current Practice

5.1 Communication

- The official school email service may be regarded as safe and secure. Staff and pupils 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 system '@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.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

- Further information is provided to staff during in service training.

5.2 Social Networking

- 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.

5.6 Teaching and Support Staff: Password Security

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.

5.7 Students: Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school’s Acceptable Use Policy

- Students are expected to keep their passwords secret and not to share with others, particularly their friends.

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

- Pupils are taught about appropriate use of passwords in Year 8.

5.7 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 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.

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

6. Pupil Guidance

Students are expected to abide by the following guidance which appears in the Pupil Planners:

- *Never use school computers in an unsupervised area*
- *Leave computer rooms tidy when you leave.*
- *Check your print credits regularly and don't let them get too low.*
- *If a lesson finishes early you should look through your file area and remove any unnecessary files to a USB drive (keep your file area as clear as possible).*
- *USB drives are really handy but they are also very unreliable and easily lost. Never keep your only copy of work on them.*
- *Your user area is backed up every night so if you accidentally delete anything it can usually be recovered (unless it was only done that day).*
- *If you keep your user area tidy it makes it easier to find things.*
- *Never access the school network using another user's password and never reveal your password to another user.*
- *Do not use school computers, or any remote computers, in such a way that you would disrupt their use by others.*
- *Do not load paper into printers or perform any similar task that a member of staff should perform (connecting / disconnecting USB devices other than your own)*
- *All communications and information accessible via the network should be assumed to be the private property of some third party.*

- *Be polite in all electronic communication (email, text, IM or similar) Remember that there is no such thing as a private email discussion on a school computer*
- *Do not access inappropriate material on any device (any material that you would not access if the Principal was sitting next to you).*
- *Personal activities on phones and other personal devices should be based on absolute necessity and only at the permitted times for having devices powered on. Pupils should not be using their mobile phones between classes and any which are used at such a time may be confiscated for the day, being collected from reception at 3.30.*
- *The school has very limited permission relating to video/photography for most students, but not all. Students photographing or video recording other students should be avoided unless instructed as part of a classroom activity.*
- *Do not send inappropriate material on any device (any material that you would not send if the Principal was sitting next to you) or any inaccurate information.*
- *Note that electronic mail (e-mail) is not private. C2k and members of school staff have access to all email and work areas.*
- *Illegal activities will be reported to relevant authorities.*
- *It will be the* **responsibility of the student** *to ensure that their actions, when using any school computers or personal devices, are appropriate and legal.*
- *Personal internet access should never be attempted on a school computer!*
- *Check MySchool for C2K's own rules and more.*

Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Anti-Bullying Policy will be implemented.

A positive attitude to the problem of bullying can bring many rewards:-

(a) *an improvement in the life of many pupils;*

(b) *an improvement in the community spirit of the school and of the caring attitude which it wishes to cultivate;*

(c) *an increase in the sense of self-worth which is so important to both pupils and staff;*

Where bullying is found to have taken place the school's policy may be to punish the bully via the normal sanctions of school discipline, but also to address the problem in a constructive manner which both assists the victim to feel more self-confident and encourages the bully to address their own problematic behaviour.