DE LA SALLE HIGH SCHOOL

DOWNPATRICK

E-SAFETY POLICY

It is the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. The guidelines set out by the Inspection and Self-evaluation framework is to ensure there is a “safe and secure environment for all members of the school community”. De La Salle is a digital technology hub through the use of iPad technology therefore relationships through technology for learning are characterised by mutual respect, openness and trust. Children and young people are able to use the internet and related communication technology appropriately and safely. These are addressed as part of the wider duty of care in curriculum class of ICT and PD. This is regularly reviewed to ensure effectiveness and flexibility and is responsive to the changing needs of technology and society for the needs of the pupils. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

De La Salle will 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.

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 technology 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 safeguarding of all involved, apply sanctions as appropriate and review procedures.

In relation to safeguarding incidents around e-safety 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 incidents outside of the School, will be dealt with in accordance with school discipline and school sanctions will apply.

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, 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.

2. Contact

• Inappropriate communication / contact with others, including strangers.

• 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, Disposal of documents.

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.

4.1 Principal/ ICT co-ordinator / Designated Child Protection Officer

The Principal and Child Protection Officer will be trained in safeguarding around electronic devices 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

• Potential or actual incidents of grooming

• Cyber-bullying

4.2 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 though the day-to-day responsibility of their care and welfare.

The Principal/Child Protection/ICT co-ordinator 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 ICT 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.

The Principal/SLT/ICT co-ordinator will monitor and review online safety policy through the 360 degree safe online framework in line with SWGfl.

4.3 Governors:

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

They will:

• have regular meetings with the Coordinators

Training will be given to the Governors by:

• Attendance at training provided by relevant external agencies / staff in school

• Participation in school's training / information sessions for staff or parents

4.4 Network Managers –C2k

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

• that C2k/Classnet operates with robust filtering and security software

• that monitoring reports of the use of C2k / Classnet 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

• that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

• that the "administrator" passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place

4.5 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, understood and signed the school's Staff Acceptable Use Policy.

• They report any suspected misuse or problem to the e-safety co-ordinator.

• Digital communications with students (email /showbie/homework app/youtube/other app) should be on a professional level only carried out using official school systems – either C2K or through 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.

• That students have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998)

• They monitor ICT activity in lessons, extracurricular and extended 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

4.6 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.

• A programme of e-safety training will be made available to staff as an integral element of CPD. Training in e-safety will be supported within the PRSD or EPD process and where staff have identified a need.

• Staff will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

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

4.7.1Pupils

Are responsible for ensuring that:

• They use the school ICT systems in accordance with the Pupil Acceptable Use Policy, 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/showbie/youtube/other apps 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.

4.7.2 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 ICT / PD / other lessons 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. This is integrated into the ICT SOW during January and February to run in line with Internet Safety Week in February.

• 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.

• Pupils will be helped to understand the need for the student AUP 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.

• Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

4.7.3 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the e-safety policy outlined by the School.

Parents and carers 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

4.7.4 Parents / Carers 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 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 and Digital Parenting

• Letters, newsletters, websites

• E-Safety Guidance will be delivered through key events

• A designated E-Safety Parents' Evening

4.9.5 Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUP before being provided with access to school systems.

4.9.6 Education for the Community

• The school will provide opportunities for members of the community to gain from the school's E-Safety knowledge and experience through:

• Providing family learning courses in use of new digital technologies, digital literacy and E-Safety

• The school website

• Supporting community groups e.g. Shared Education/sports/voluntary groups to enhance their E-Safety provision

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 systems '@c2kni.net' or @ xxxxxxxx . 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 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. (Please see the School Social Media Policy)

• Further information is provided to staff during in service training

5.2 Social Networking

At present, the school endeavours to deny access to social networking sites to pupils during school hours. Staff may use Twitter / You Tube to disseminate information to pupils outside of school.

• The school will provide training in the appropriate use of social networking / for teaching and learning purposes.

• Training will include: 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.

• Teachers will receive training in the appropriate use of social networking in their private life

• Pupils over 13 years of age 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.

• Further information is provided to staff during in service training, also see the 'Social Media Policy' for appropriate use.

5.3 Pupils' use of personal devices

• The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

Mobile phones are not permitted to be used in school

• Mobile Phones and personally-owned devices must be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

• If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

• In accordance with JCQ regulations, phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

• Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in 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 will 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, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

• Further information is provided to staff/pupils/parents during in service training, also see the 'Mobile Devices Policy' for appropriate use.

5.4 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety.

We will not reveal any recordings, without permission, except where disclosed to the Police as part of a criminal investigation.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5.5 Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

• When using digital images, staff informs and educates 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 agreement form when their son joins the school;

• 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 images.

• We will also ensure that when images are published that the young people 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.

• The school will comply with the Data Protection Act by requesting parents' permission when their child starts school Year 8, permission will last until the student leaves school, unless a parent / carer provides a written withdrawal of taking images of members of 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.

• Further information is provided to staff during INSET training, also see 'Passwords - Safe Practice Guidance Sheet'

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.

5.8 The Data Protection Act

The school has a Data Protection Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they:

• at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

• transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media, it is advisable that:

• the device is password protected

• the device offers approved virus and malware checking software

• the data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete

5.9 Google Apps for Education

The school uses Google Apps for Education for pupils and staff. The following services are available to each pupil and hosted by Google as part of the school's online presence in

Google Apps for Education:

• Mail - an individual email account for school use managed by the school

• Calendar - an individual calendar providing the ability to organise schedules, daily activities, and assignments

• Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

• Sites - an individual and collaborative website creation tool

As part of the Google terms and conditions schools are required to seek parental permission for your child (under 13 years old) to have a Google Apps for Education account which will be sought at the beginning of Year 8.

5.9.1 Technical Framework

Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school's filtering policy is held by Senior Leadership Team.

They manage the school filtering by:

• Monitoring reports of the use of C2k which are available on request.

• Keep records and logs of changes and of breaches of the filtering systems.

• These changes and breaches should be reported to the Principal

Staff and pupils have a responsibility:

• to report immediately to e-safety 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.

• Users 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.

7. Actions and Sanctions

Sanctions for the misuse of technology are outlined in the Behaviour Policy.

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) Violation of the rules will result in a temporary or permanent ban on Internet and iPad technology

b) Additional disciplinary action may be added in line with existing school rules on inappropriate language or behaviour.

c) Where applicable, police or local authorities may be involved.

7.1. Acceptable Use of Digital Images of Pupils

All staff should follow the guidance below when dealing with taking, display storage and use of photographs and digital images of pupils.

Taking of Photographs/Video of Pupils

Staff should continue normal practice. Parents will be informed in writing and asked to give their consent to a range of such activities. Staff will be advised of those parents who withhold permission in due course.

Display/use of Photographs/Video of Pupils

Staff should continue normal practice for using photographs for display purposes in school. For displays/use outside school or where staff require additional guidance on the display/use of photographs the Principal or a member of the SMT **should be consulted**.

7.2 Storage of Photographs/Video of Pupils

It should **not be** normal practice to store digital images of pupils (however obtained) on school or personal ipads/laptops as a matter of course for **prolonged** periods of time. As a result staff should ensure that:

1. Any image/s of a pupil/s (from camera, ipad or other source) that is/will be stored digitally and should be stored on CD-ROM or on the C2k Private folders. Technical support will be available from the ICT department to assist in the transfer of existing/new images to CD-ROM.

2. After initial use by staff digital images of pupils should be **deleted from laptops/iPads as soon as possible.**

3. Staff should not pass images of students via e-mail, CD-ROMs etc to third parties without consulting the Principal

4. Traditional photographs of pupils should continue to be stored within departments using scrapbooks or a suitable alternative.

If you require further advice consult the Principal or a member of the SLT. This guidance will be reviewed on an annual basis.

Additional Advice for Parents with Internet access at Home

1. The iPad/computer with Internet access should be situated in a location where parents can monitor access to Internet. Computers should be fitted with suitable anti-virus, anti-spyware and filtering software.

2. Parents should agree with their children suitable days/times for accessing the Internet. If using dial-up accounts, Internet usage can add significantly to your phone bill. Off-peak calls (after 6pm daily and weekends) are cheaper, but the cost of Internet access still needs to be carefully considered. Fixed-price broadband services represent the best value for money.

3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use;

4. Parents should get to know the sites their children visit, and talk to them about what they are learning;

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available below.

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school or by C2k, they should immediately inform the school.

Further free advice for parents is available from the following sources:

http://www.thinkuknow.co.uk/ - a website designed to inform children of the potential hazards involved with online chatrooms.

www.kidsmart.org.uk – a website designed to promote safe use of the internet

http://www.getnetwise.org/ - information about filtering programs for home use

Protecting Your Home Computer

To protect you home computer, parents are advised to ensure the following items of software are installed on their home computers:

- **Anti Virus Software:** free anti-virus software is available from a range of software suppliers e.g. AVG
- **Anti Spyware Software:** free anti-spyware software can be installed on all home computers. Use Google to find a suitable package e.g. Advanced System Care or Malware Bytes.
- **Filtering Software:** free filtering software is provided by by a range of suppliers e.g. K-9 Bluecoat filtering software www.k9webprotection.com/

Appendix 2 – Social Networking Code of Conduct

Social networking websites and Communication Technology

Guidelines for a Code of Conduct for those who work with children and young people.

Social Networking

Social networking is everywhere. It is common to find parents, children, co-workers and others on such sites. With social networks people across the world have access to tools and options that were previously non-existent. However, there are now just as many new opportunities to connect as there are to get into potential danger. One thing we often forget while having fun on social networks is that almost anybody can see what we are doing. While we are tagging photos for our friends or are posting comments to them, it can be easy to forget that someone else who has been invited onto a social networking site can also view them.

Once something appears on the Internet, it's almost impossible to remove. As these sites continue to grow in popularity, so too does the value of the information on them to parties other than those directly involved. Social networking users need to take a step back and think about just what they're posting onto the Internet.

Guidelines

The following guidelines should be read in conjunction with the Code of Conduct for your service, school or organisation.

People who work with children and young people should always maintain appropriate professional boundaries, avoid improper contact or relationships and respect their position of trust.

With regard to relationships, individuals who work with children and young people should not attempt to establish an inappropriate relationship which might include:

- communication of a personal nature
- inappropriate dialogue through the internet
- the sending of emails or text messages of an inappropriate nature

Individuals, who work with children and young people, should be extremely careful in corresponding with people on social networking sites. Staff relationships with children and young people should at all times remain professional and they should **not** correspond with children and young people through such sites or add them as 'friends'. It is worth bearing in mind that on such sites an inappropriate or even misconstrued communication may have the potential to impact upon their careers or even result in criminal investigation.

In addition staff should bear in mind who may access their own profiles on such websites and should therefore take care as to the information they display about themselves and their personal lives. They should also ensure that they have installed and are using the appropriate privacy settings.

Individuals, who work with children and young people, should not make, view or access illegal or inappropriate images of children.

Individuals, who work with children and young people and others, with whom they may be in a position of trust, should exercise caution when using social networking sites and avoid inappropriate communication of any kind.