De La Salle College

Signum Fidei

Online Safety Policy

Under Review

This policy has been reviewed in line with DENI circulars 2016/27 Online Safety and 20/15/21 School Obligations – Information Governance and C2k Access to SIMS Data.
December 2017

Contents

Introduction 4
Roles and Responsibilities 6
Online Safety skills development for staff 7
Managing the school Online Safety messages 7
Online Safety in the Curriculum 7
Password Security 9
Data Security 10
Managing the Internet 11
Infrastucture 11
Managing other Web 2 technologies 14
Mobile technologies 16
Personal Mobile devices (including phones) 16
School provided Mobile devices (including phones) 17
Managing email 18
Safe Use of Images 20
Taking of Images and Film 20
Consent of adults who work at the school 20
Publishing pupil's images and work 21
Storage of Images 21
Webcams and CCTV 22
Video Conferencing 22
Misuse and Infringements 24
Complaints 24
Inappropriate material 24
Pupils with special educational needs. 25
Parental Involvement 26
Writing and Reviewing this Policy 28
Staff and pupil involvement in policy creation 28
Review Procedure 28
Acceptable Use Agreement: Staff, Governors and Visitors 29
Staff, Governor and Visitor 29
Acceptable Use Agreement / Code of Conduct 29
Pupil Acceptable Use 31
Agreement / Online Safety Rules 31
Parental Consent Letter 33
Flowcharts for Managing an Online Safety Incident 34
Incident Log .... **Error! Bookmark not defined.**
Current Legislation 37
Other Acts relating to Online Safety 38

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 Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced 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
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile / Smart phones with text, video and / or web functionality
- Other mobile devices with web functionality

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

At De La Salle College, we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom. Safeguarding and promoting pupils’ welfare around digital technology is the responsibility of everyone who comes into contact with them in De La Salle College or on school organised activities.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, 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, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

Children and young people have a right to be protected and educated. De La Salle College has the responsibility to take appropriate preventative action to protect children and minimise the associated risks around online safety. These risks have been defined under four categories.

- **Content risks:** The child or young person is exposed to harmful materials.
- **Contact risks:** The child or young person participates in adult-initiated online activity and / or is at risk of grooming.
- **Conduct risks:** The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and / or is at risk of bullying, entrapment and / or blackmail.
- **Commercial risks:** The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs / fraud.

As Online Safety is an important aspect of strategic leadership within the school, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety Coordinator in our school is Mr John Tohill 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 Online Safety Coordinator to keep abreast of current issues and guidance through organisations such as EA, DENI, Ineqe Group, Naace, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Principal / Online Safety Coordinator 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, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following school policies: Child protection, Positive Behaviour, Social Media, Use of Email, Anti-bullying and Teaching and Learning.

Online Safety skills development for staff

- Our staff receive regular information and training on Online Safety issues in the form of regular communication through email, whole staff briefings, ICT workshops and departmental meetings.
- Details of the ongoing staff training programme can be found in the staff handbook and through the staff documents area of the school network.
- New staff receive information on the school’s acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

Managing the school Online Safety messages

- We endeavour to embed Online Safety messages across the curriculum. whenever the Internet and/or related technologies are used.
- The Online Safety policy will be introduced to the pupils at the start of each school year.
- Online Safety posters will be prominently displayed.
- Online Safety information will be displayed beside every device in the school.

Online Safety in the Curriculum

- The school has a framework for teaching Internet skills in ICT / PSE lessons.

- The school provides opportunities within a range of curriculum areas to teach about Online Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum in PSE lessons.
- 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 and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of cyber bullying and know how to seek help if they are affected by these issues. 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 Childline / 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.

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.
- Users are provided with an individual C2K log-in username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to Mr J Tohill or an ICT technician.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and / or Learning Platforms, including ensuring that passwords are not shared and are changed regularly. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into any virtual learning environment (VLE) such as Studywiz, Fronter or google classroom.
- In our school, all ICT password policies are the responsibility of the ICT Technician and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing of school data is something that the school takes very seriously. The school follows Naace guidelines (published Autumn 2008) and the guidelines outlined in circular 2015/21.

Staff are aware of their responsibility when accessing school data. They must not;

- access data outside of school, except when using a device owned by the school.
- take copies of the data.
- allow others to view the data.
- edit the data unless specifically requested to do so by the Principal and / or Board of Governors.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. **All use of the C2k network and Internet access is logged** and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school ensures students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils although access is given to image searches.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- The school will be installing SECURUS software in early 2018 to further enhance online safety.
    - Appropriate training and education for staff and pupils regarding SECURUS will be delivered to all members of the school community.

Infrastucture

- Because of an identified need for an alternative Internet access in addition to C2K's filtered Internet service, there are two separate filtering systems in place.

- For C2K managed devices, school Internet access is controlled through C2K's web filtering service. For further information relating to filtering please go to www.c2kexchange.org.uk
- For non-C2K managed devices, the responsibility for the effective filtering of any inappropriate content rests with the Board of Governors.
    - All non-C2k devices have OpenDNS filtering software installed.
    - This software allows the school to black-list particular sites as required.
    - For all school tablets, especially iPads, Internet access is disabled by default. For these a devices, a "opt-in" or white list of websites is maintained. This means that pupils can only accessed websites tested and recommended by the class teacher.
- De La Salle College is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the Online Safety Coordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's nor the network manager's responsibility to install or maintain virus protection on personal systems.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Online Safety Coordinator.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed directly or by email.

Managing other Webtechnologies

Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative and free facilities. They provide an excellent vehicle for communicating directly with parents/ craers and the wider community. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school policy is to deny access to social networking sites to pupils within school using their own personal accounts.
- Students using social networking sites such as Twitter are required to create an account specifically for this purpose using their C2k email address to register these accounts.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile / home phone numbers, school details, IM / email address, specific hobbies / interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are educated in relation to the appropriateness of communication with school social media sites.
- Our pupils are asked to report any incidents of cyber bullying to the school.

- Staff may only create blogs, wikis or other any other Internet based resource in order to communicate with pupils using systems approved by the Principal or Online Safety Coordinator.
- Further information can be found in the school’s Social Media Policy.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent / carer using their personal device.
- Pupils are allowed to bring personal mobile devices, including mobile phones to school.
- This technology may be used, however for educational purposes, as mutually agreed with the Principal and Online Safety Coordinator. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Only the school provided tablet pc or iPad for staff, should be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good ‘netiquette’. This section should be read in conjunction with the School Email policy.

- The school gives all staff their own C2K email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using the staff member’s personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, ‘the views expressed are not necessarily those of the school. The responsibility for adding this disclaimer lies with the account holder.
- E-mails sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Principal, line manager or designated account.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of

appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

- Pupils must immediately tell a teacher / trusted adult if they receive an offensive e-mail.
- Staff must inform the Online Safety Coordinator / line manager if they receive an offensive e-mail.
- Pupils are introduced to email as part of the year 8 ICT Scheme of Work.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are discouraged from using personal digital equipment, such as mobile phones and cameras, to record images of pupils; this includes when on field trips. However, with the express permission of the Principal or Online Safety Coordinator, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others; this includes when on field trips.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing pupil's images and work

On a child's entry to the school, all parents / guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site and official school social media accounts.
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded / transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

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, e.g. divorce of parents, custody issues, etc.

Parents / carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' full names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

Storage of Images

- Images / films of children are stored on the school's network and backed up using C2K .

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Online Safety Coordinator.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network / Learning Platform.
- Mr J Tohill and Mr P Buchanan have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Principal and other staff designated by the Principal. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the "inappropriate materials" section of this document)
    - Webcams can be found in the ICT manager's office. Notification is given in this/these area(s) filmed by webcams by signage.
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants.

- Approval from the Principal is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Misuse and Infringements

Complaints

Complaints relating to Online Safety should be made to the Online Safety Coordinator or Principal. Incidents should be logged and the Flowcharts for Managing an Online Safety Incident should be followed (see appendix).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety Coordinator, depending on the seriousness of the offence; investigation by the Principal, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct through the acceptable use document and conduct policy

Equal Opportunities

Pupils with special educational needs.

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents / carers and pupils are actively encouraged to contribute to adjustments or reviews of the school Online Safety policy**.**
- Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to Online Safety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website / Learning Platform postings
    - Newsletter items
    - Learning platform training

Monitoring and Evaluation

From December 2017, the school maintains an up-to-date record of potential breaches of online safety in an Online Safety Risk Register.

Access to SIMS modules for individual members of staff can only be approved by the Principal or the Online Safety Coordinator.

An up-to-date register of SIMS access is held within the school and is currently maintained by the Online Safety Coordinator.

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

Staff and pupils have been involved in making / reviewing the Online Safety policy through SLT meetings, Departmental meetings and the school council.

Review Procedure

There will be an on-going opportunity for staff to discuss with the Online Safety coordinator any issue of Online Safety that concerns them.

This policy will be reviewed every 3 years and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, Principal and governors on………………………………

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of ICT. All members of staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr J Tohill, De La Salle College Online Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning NI and any related technologies for professional purposes or for uses deemed "reasonable" by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors.
- I will not install any hardware of software without permission of the ICT manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent / carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .... Date ....

Full Name .... (printed)

Job title ....

Acceptable Use Agreement: Pupils

Pupil Acceptable Use Agreement / Online Safety Rules

- I will only use ICT systems in school, including the Internet, email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network / Learning Platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address in school.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not deliberately play computer games except where assigned by a teacher for educational purposes.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone through using ICT.
- Images of pupils and / or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission of the Principal.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the Internet filtering system.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature .... Date ....

Full Name .... (printed)

Parental Consent Letter

Dear Parent/ Carer

ICT including the Internet, learning platforms, email and mobile technologies has become an important part of learning in our school.   We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of Online Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Mr J Tohill, De La Salle College Online Safety coordinator.

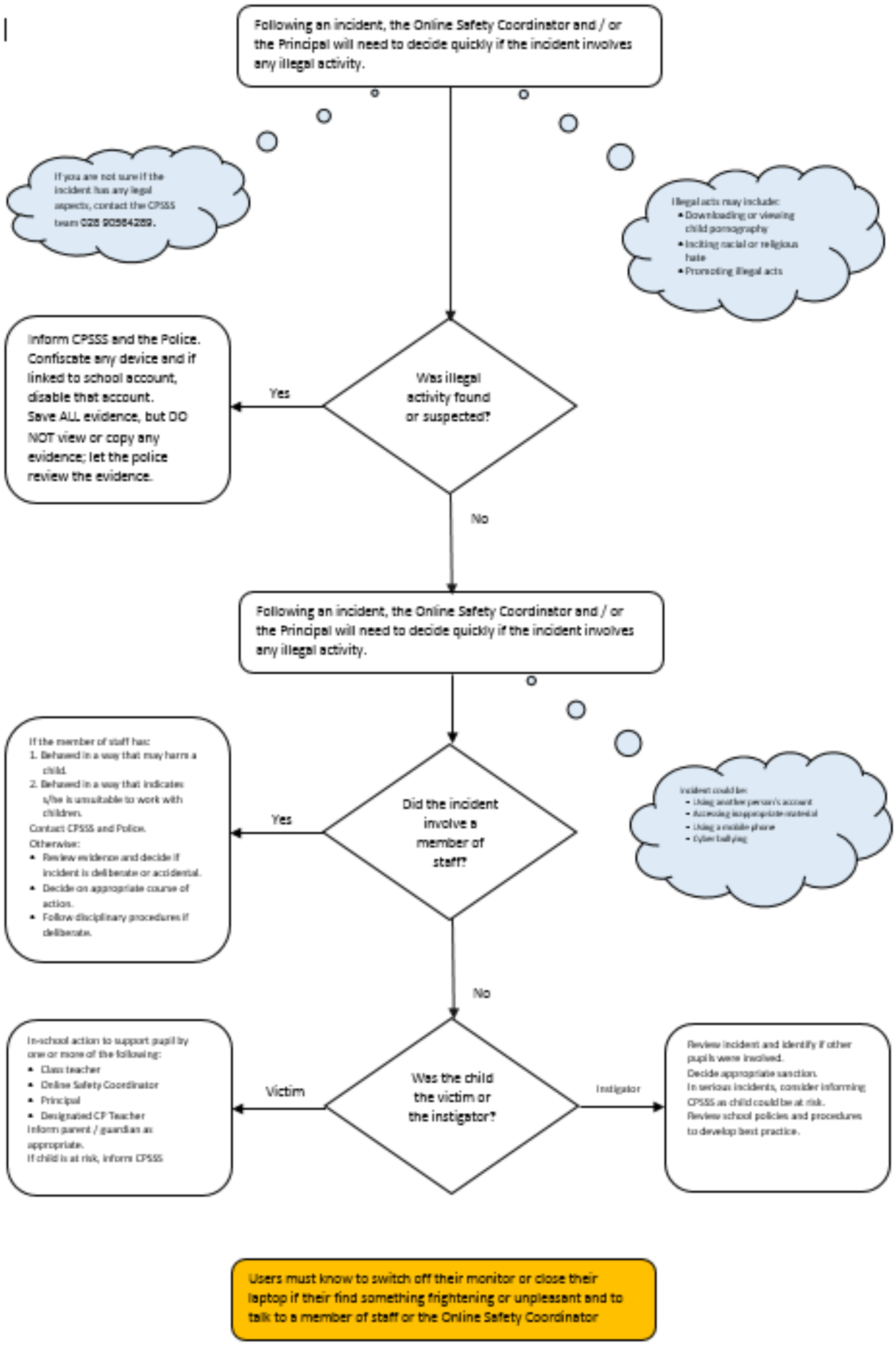
Please return the bottom section of this form to school for filing.

✂

Pupil and Parent/ carer signature
We have discussed this document and ……………………………………..........(pupil name) agrees to follow the Online Safety rules and to support the safe and responsible use of ICT at De La Salle College.
Parent / Carer Signature …….……………………………………………
Pupil Signature……………………………………………………………….

Form ………………………………… Date ……………………………

Flowcharts for Managing an Online Safety Incident


Following an incident, the Online Safety Coordinator and / or the Principal will need to decide quickly if the incident involves any illegal activity.
If you are not sure if the incident has any legal aspects, contact the CPSSS team 028 90564289.
Illegal acts may include:
• Downloading or viewing child pornography
• Inciting racial or religious hate
• Promoting illegal acts
Was illegal activity found or suspected?
Yes
Inform CPSSS and the Police. Confiscate any device and if linked to school account, disable that account. Save ALL evidence, but DO NOT view or copy any evidence; let the police review the evidence.
No
Following an incident, the Online Safety Coordinator and / or the Principal will need to decide quickly if the incident involves any illegal activity.
Incident could be:
- Using another person's account
- Accessing inappropriate material
- Using a mobile phone
- Cyber bullying
Did the incident involve a member of staff?
Yes
If the member of staff has:
1. Behaved in a way that may harm a child.
2. Behaved in a way that indicates s/he is unsuitable to work with children.
Contact CPSSS and Police.
Otherwise:
• Review evidence and decide if incident is deliberate or accidental.
• Decide on appropriate course of action.
• Follow disciplinary procedures if deliberate.
No
Was the child the victim or the instigator?
Victim
In-school action to support pupil by one or more of the following:
• Class teacher
• Online Safety Coordinator
• Principal
• Designated CP Teacher
Inform parent / guardian as appropriate.
If child is at risk, inform CPSSS
Instigator
Review incident and identify if other pupils were involved.
Decide appropriate sanction.
In serious incidents, consider informing CPSSS as child could be at risk.
Review school policies and procedures to develop best practice.
Users must know to switch off their monitor or close their laptop if their find something frightening or unpleasant and to talk to a member of staff or the Online Safety Coordinator

Online Safety Risk Register

Details of ALL online safety incidents to be recorded by the online safety Coordinator. This incident log will be monitored termly by the principal, members of SLT or the chair of the Board of Governors. Any incidents involving bullying or child protection will additionally be logged in the appropriate log.

Date and time	Name of pupil or staff member	Gender	Room and device number	Details of incident (including evidence)	Actions

.

Smile and Stay Safe Poster

Online Safety Rules to be displayed next to all PCs in school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to Online Safety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on

conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:
access to computer files or software without permission (for example using another persons password to access files)
unauthorised access, as above, in order to commit a further criminal act (such as fraud)
impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.