St Malachy's College

eSafety Policy

Table of Contents

1. Rationale

New and emerging technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other technologies are powerful tools, which open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school.

"The rapidly changing nature of the internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. The school's e-Safety policy must reflect this by keeping abreast of the changes taking place. Schools have a duty of care to enable pupils to use online systems safely"

"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 College 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.

2. Scope of the Policy

This policy applies to **all** members of the College community who have access to and are users of the school ICT systems, both in and out of the College. In relation to incidents that occur during school hours, we will work with parents, staff and students 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 College 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 College 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 College, will be dealt with in accordance with College 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 College 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.
- 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 and information 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 College 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. Roles and Responsibilities

Governors:

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

The designated e-Safety Governor is Mr. F McElhatton. He will:

- Meet with the e-Safety Officers
- Monitor e-Safety incident logs

Training for Governors may be offered through:

- Attendance at training provided by relevant external agencies
- Participation in school's training / information sessions for staff or parents

Principal and Senior Leaders:

The Principal (Mr McBride) is responsible for ensuring the safety (including e-Safety) of members of the school community though day-to-day responsibility for e-Safety will be delegated to the e-Safety Officers. The Principal 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.

e-Safety Officers

The role is shared between the two Vice Principals; Mrs L Stewart is also C2K Manager and the other VP, Mrs D McCusker is the Designated Teacher for Child Protection.

The e-Safety Officers will:

- Lead the e-Safety committee
- Take day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the College e-Safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Provide training and advice for all staff
- Liaise with C2K, Iteach and school ICT technical staff
- Receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments
- Meet regularly with e-Safety Governor to discuss current issues, review incident logs

School Network Managers

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

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 College Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the e-Safety Officers.
- 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 St Malachy's Gmail accounts. Emails should be sent in accordance with the College's guidance.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- 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
- They undertake all e-Safety training as organised by the College

Students

Are responsible for ensuring that:

- They use the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to the College's 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 College 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
- They understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the College's e-Safety Policy covers their actions out of school, if related to their membership of the school.

e-Safety Committees

Staff e-Safety Committee – Teachers and Support Staff

Will assist the e-Safety Officers with:

- issues regarding e-safety
- the production / review / monitoring of the school e-Safety policy/documents and initiatives.
-

Committee Members

- e-Safety Officers (includes Designated Child Protection Officer and C2K Manager):
- ICT Staff
- Staff Digital Leader
- Head of ICT (Mr Crozier) and Mrs Mulholland (KS3 Using ICT)
- Heads of School:
- e-Safety Governor

Student e-Safety Committee

The student e-Safety committee (sub-committee of the School Council) will assist the e-Safety Officers with:

- Potential issues regarding e-safety
- Presenting information during an assembly on the Safer Internet Day
- Contributing to staff committee meetings where deemed relevant.

5. Training and Development

e-Safety Governor

- Will be trained in e-Safety issues and be aware of the potential for serious Child Protection issues.

Principal and Senior Leaders

- Will be trained in e-Safety issues and be aware of the potential for serious Child Protection issues.

e-Safety Officers / Designated Child Protection Officer / Designated Deputy Child Protection Officer

- Will receive regular updates through attendance at ELB and other relevant information training sessions and by reviewing guidance documents released by DENI and others. They will also avail of CEOP Training where appropriate.
- 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
- Potential or actual incidents of grooming
- Cyber-bullying

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.

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

Students

e-Safety education for students will be provided in the following ways:

- A planned e-Safety programme will be provided as part of ICT / PHSE / 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.

- Students 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.

- Students will be helped to understand the need for the student Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

Parents / Carers

Parents and carers are responsible for their son's e-Safety outside the school and should work with the College to support the e-Safety Policy.

The College 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

- E-Safety Guidance will delivered through key events

- A designated e-Safety Parents' Evening

6. Current Practice

6.1 Technical - Infrastructure / equipment, filtering and monitoring

The College, through C2k and Classnet will be responsible for ensuring that the schools' network is safe and secure as is reasonably possible and that policies and procedures are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.

The 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.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the c2k co-ordinators. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to the e-Safety Officers.

All users have a responsibility to report immediately to e-Safety Officers 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.

C2k filtering

Staff and pupils accessing the Internet in school via C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network Solution. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the Principal.

Classnet filtering

Staff and students will access the Internet using their iPad on the Classnet network. This will automatically be authenticated using a 'Profile' on the iPad which is installed during iPad set up. Each iPad should be protected by a passcode set as outlined in the College's Staff / Student Acceptable Use Policy. Access to the Internet via the Classnet network is fully auditable and reports are available to the Principal.

This filtration service uses a category based system to decide if a website is viewable from all Internet connected devices.

The primary categories include:

- Child Protection (including violence, porn, weapons etc)
- Leisure (entertainment, travel, sports)
- Business
- Chatting (internet chatting and instant messaging services)
- Computer & Internet Services (social networking, streaming, spam sites)
- Other (image sharing, dating and person, compromised, inc uncategorised)

If a website falls into a category that is not deemed acceptable for use in the classroom, the user will be subject to viewing an "unsuitable" notification on the web browser and this activity logged to user and device level. Cyren independently searches the Internet using their tools to select what category is assigned to any available website. This is then matched to the live filtering within the school.

To enhance category based filtering:

- Standard browsers are removed (e.g. Safari) and is replaced by a secure browser which adds a second filtering level per device. This is controlled on age based settings and is secondary to the firewall filtering. No pupil can access an unfiltered browser.
- All devices are supervised which enables Internet access control at OS level, which offers a final layer of filtering based in content groups and discrete Internet addresses.
- The College maintains a rolling list of websites requested by teaching staff, checked and approved to be exempt from category filtering and this available in school. This list is maintained by the ICT technician and relevant e-Safety coordinator. Websites are added to a specific blocking list where and when required.

College Procedures

- The College has a mechanism should a website be found to be uncategorised, and can request a category to be allocated from within the URL category tool.
- Individual websites and iOS apps can be permitted through the filtering system on a site per site basis using a system called White Listing. This is used when blocking such apps as Twitter, Facebook and Tumblr that operate within an 'App' environment.
- Filtering has been checked by two senior staff within Department Guidelines.
- Two members of staff have been trained in filter use in order to respond to any system issue.
- The network is supported on demand from an external agency (iTeach).

Education

Students/ 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.

Monitoring

Any filtering issues should be reported immediately to the filtering provider. Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- e-Safety committee
- e-Safety Governor
- e- Safety Officers
- External Filtering provider / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

Email

Teaching and Support Staff

Email communications with parents and/or students, if deemed necessary, should be conducted through the following school email systems **'@c2kni.net'** or **'@stmalachyscollege.org'**. Staff should **not** contact students, parents or conduct any school business using personal email addresses. Furthermore, the school email account should be used for school related business only. It is important to note that all email accounts may be subject to scrutiny by the College through the filtering and monitoring facilities.
Further information is provided to staff during INSET training. For more detailed guidance, see Staff Acceptable Use Policy

Students

- Students can use C2K mail, and / or Google mail with parental consent.
- Students are introduced to, and use e-mail as part of the ICT curriculum
- Students are taught about the safety and 'netiquette' of using e-mail both in school and at home

Students' use of personal devices

- The College accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a College 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.
- If a student needs to contact his or her parents or carers, this will be facilitated through the College switchboard. Parents should not contact their child via their mobile phone during the school day and should make contact via the College office if necessary.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students 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 use of personal devices

- Personally owned mobile phones devices will 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.
- 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.

Social Networking

At present, the College endeavours to deny access to social networking sites to students within school. However, staff may use Twitter / You Tube to disseminate information to students outside of school.

- Teaching staff can avail of training in the appropriate use of social networking / for teaching and learning purposes

- Teachers should adhere to the social networking / communication guidance provided by the College

- Teachers will receive training in the appropriate use of social networking in their private life
- Older students should be made aware of the appropriate and safe use of Social Networking
- Teachers and students should report any incidents of cyber-bullying to the school

VLE

- Uploading of information on the College's VLE is shared between different staff members according to their subject area and responsibilities. Content should be monitored by the HOD.

- Photographs and videos uploaded to the College's VLE will only be accessible by members of the school community.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), 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 good examples best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

School website

- The Website co-ordinator takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status

- The point of contact on the website is the school address and telephone number and we use a general email contact address

- Photographs published on the web do not have full names attached
-

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 College Anti-Bullying Policy.

Passwords

Teaching / Support Staff

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 they are are locked.
- Further information is provided to staff during INSET training, also see 'Passwords - Safe Practice Guidance Sheet'

Students

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

Digital and video images

Staff, parents and students need to be aware of the risks associated with taking digital images and sharing on the Internet.

- When using digital images, staff should inform and educate students 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 College 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.
- Students must not take, use, share, publish or distribute images of others without their permission.

- The use of digital / video images plays an important part in learning activities.

- The College 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.

Google Apps for Education

The College uses Google Apps for Education for students and staff. The following services are available to each student 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

Using these tools, students collaboratively create, edit and share files and websites for school related projects and communicate via email with other students / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer.
Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others. The College believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions schools are required to seek your permission for your child to have a Google Apps for Education account which will be sought at the beginning of Year 9.

Unsuitable and inappropriate activities

In accordance with Staff School Acceptable Use Policies, Internet activity relating to for example child abuse images or distributing racist material is illegal and consequently banned from school systems.

Staff must be professional in their use of the school system and not access or permit students to access any inappropriate material.

If there is any suspicion that that the website(s) concerned may contain
child abuse images, or if there is any other suspected illegal activity, refer to the flowchart (appendix 1) for responding to online safety incidents and report to the police.

Schedule for Developing, Monitoring and Reviewing Policy

Approval by the Board of Governors 11 February 2015

The implementation of this e-Safety policy will be monitored by:

The e-Safety Officers

Monitoring and reviewing:

Annually, and only if required following a breach of safety.

The Board of Governors will receive regular reports on e-Safety including anonymous details of e-Safety incidents:

This will be in conjunction with the Child Protection Report, presented by the VP to the Board of Governors.

Should serious e-Safety incidents take place, the following external persons or agencies should be informed:

Gateway Team
BELB
PSNI
Chair of BoG

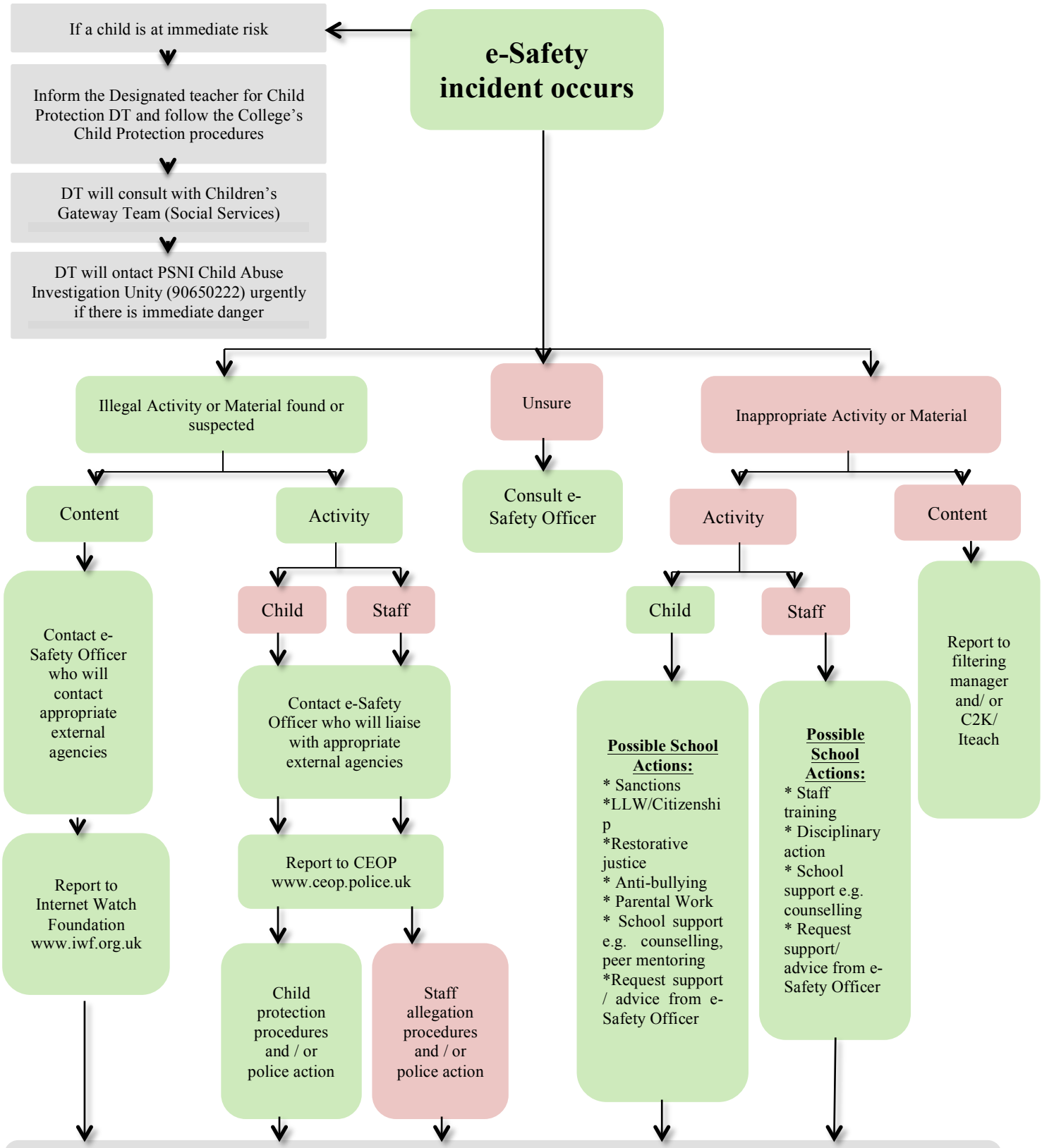
This policy has been agreed and formally adopted by the Board of Governors of St Malachy's College, Belfast.

Signature: _____ Date : _____
(Chairperson of the Board of Governors)

Signature: _____ Date : _____
(Principal)

Next Review Date : _____

Appendix 1 Response to an Incident of Concern



Local Contact Details:

Schools Designated Teacher for Child Protection: Mrs D McCusker/ Deputy DTs: Mrs S Rayot/ Mr F Toner/ Mrs M O'Neill
School's e-Safety Co-ordinator: Mrs L Stewart (VP/C2k co-ordinator) and Mrs D McCusker (Designated Teacher
E-Safety / Child Protection Governor(s): Mr F McElhatton
PSNI Child Abuse Investigation Unit: 028 90650222

iPad Policy Agreement Form

Please complete and return to Form Tutor.

I accept and will adhere to the guidelines and conditions outlined in the iPad Acceptable Use Policy.

Student Section:

Name of Student: ..... (Block Capitals)

Form Class: .....

Pupil Signature: .....

Date: .....

Parent/Guardian Section:

I have read and agree to the conditions outlined in the iPad Acceptable Use Policy.

Name of Parent/Guardian: .....
(Block Capitals)

Relationship to student: ……..

Parent/Guardian Signature: .....

Date: .....

Appendix 3

Use of Cloud Systems Permission Form

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent' for their children to be able to use these services. It is suggested that schools will incorporate this into their standard acceptable use consent forms sent to parents each year.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses Google Apps for Education for *students* and staff. This permission form describes the tools and pupil / student responsibilities for using these services.

The following services are available to each s*tudent* 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 organize 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

Using these tools, *students* collaboratively create, edit and share files and websites for school related projects and communicate via email with other students / students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to my child using the school using Google Apps for Education.

Signed

Date