PRIORY INTEGRATED COLLEGE HOLYWOOD

accomplishing more together

SCHOOL POLICY

Policy Name:	E Safety
Review date:	April 2023
Date to be reviewed:	April 2026
Agreed by the BOG on:	30th May 2023
Policies which are linked to this policy:	Safeguarding and Child Protection, Pastoral Care, Teaching and Learning, Discipline and Positive Behaviour

Integrated Education has been one of the most significant social developments within Northern Ireland in the last 40 years. Priory wears its Integrated ethos and practice with pride, Integration is prioritised by school leadership and is led by the Principal, BOGs and a drive team, under the leadership of the newly appointed Integration Co-ordinator. The four core principles of integrated education - **equality, faith and values, parental involvement** and **social responsibility** are central in all we do. Integration and Inclusion remains high on the agenda of the college and we will endeavour to make sure that every child is welcomed and taught in a safe and nurturing Priory College.

College Mission Statement

Priory Integrated College welcomes children from all traditions, cultures and abilities. Together, we aim to empower every child to reach their full potential, in a nurturing, caring environment which upholds respect and excellence for all.

E SAFETY POLICY

Purpose of the Policy

This policy focuses on three core areas:

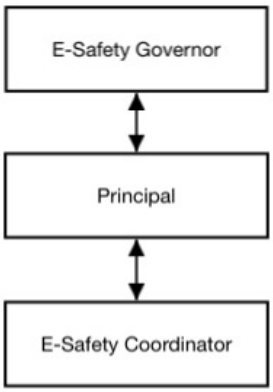
- Pupil Care
- Staff Care
- Effective and efficient use of resources

Scope of the Policy

This policy applies to all members of the College community (including governors, staff, students / students, volunteers, parents / carers, visitors, community users) who have access to and are users of College ICT systems, both in and out of the College.

Roles and Responsibilities

RESPONSIBILITY HIERARCHY



BOARD OF 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. A member of the Governing Board has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator.
- regular monitoring of e-safety incident logs.
- regular monitoring of filtering / change control logs.
- reporting to relevant governor committee groups.

PRINCIPAL AND SENIOR LEADERS

The Principal has a duty of care for ensuring the safety (including e-safety) of members of the College community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

- the Principal and (at least) another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- the Principal/ Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- the Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-SAFETY COORDINATOR

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-safety policies/ documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with the Department of Education/ SEELB.
- liaises with College technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering.
- attends relevant meeting.
- reports regularly to Senior Leadership Team.

C2K MANAGER/ TECHNICAL STAFF

- that the College's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the College 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 updated on a regular basis.
- 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 the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal/ E-Safety Coordinator for investigation.

TEACHING AND SUPPORT STAFF

- they have an up to date awareness of e-safety matters and of the current College e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Principal or E-Safety for investigation.
- all digital communications with students/ parents/ carers should be on a professional level and only carried out using official College systems.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other College activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

CHILD PROTECTION/ DESIGNATED TEACHER

should be trained in e-safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

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

STUDENTS

- are responsible for using the College digital technology systems in accordance with the Student E-Safety Charter.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking/ use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's E-Safety Policy covers their actions out of College, if related to their membership of the College.

PARENTS/ CARERS

Parents/ Carers play a crucial role in ensuring that their children understand the need to use internet and mobile devices in an appropriate way. The College will take every opportunity to help parents understand these issues through parents' evenings, letters, website / VLE and information about e-safety campaigns. Parents and carers will be encouraged to support the College in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at College events.
- access to parents' sections of the website.
- their children's personal devices in the College.

EDUCATION

Whist regulation and technical solutions are very important, their use must be balanced by education. The education of students, parents and staff is therefore an essential part of the College's e-safety provision.

STUDENTS

Children and young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- students should be taught in all lessons to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy of information.
- students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

PARENTS/ CARERS

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. 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 College will therefore seek to provide information and awareness to parents and carers through:

- Letters, website, VLE.
- Parents evenings/ awareness events.
- High profile events/ campaigns eg Safer Internet Day.

STAFF

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- all new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the College e-safety policy and Acceptable Use Agreements.
- the E-Safety Coordinator will provide advice, guidance and training to individuals as required.
- staff should understand that phone or digital communications with students can occasionally lead to misunderstandings or malicious accusations. Staff must take care always to maintain a professional relationship.

COMMUNICATION

When using communication technologies the College considers the following as good practice:

- The official College email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- users must immediately report, to the C2K Manager/ ICT Technician, the receipt of any communication that makes them feel uncomfortable, or which they feel is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.)
- Any digital communication between staff and students or parents/ carers (email, chat, VLE, Video conferencing etc) must be professional in tone and content.
- Incoming emails from an unknown source should be treated as suspicious and attachments not opened.
- In digital communications students must not reveal their personal details or those of others, or arrange to meet anyone without permission of a parent/ carer.

SOCIAL NETWORKING

All Colleges have a duty of care to provide a safe environment for students and teachers. The College provides the following measures to ensure the safety of all:

- Students are unable to access social networking sites like Facebook/ Twitter through the C2K network or private wifi system.
- Teachers who obtain knowledge of students accessing social networking sites via proxy avoidance measures should report this to the ICT Technician immediately to have the site blocked.
- College Vimeo, Facebook, Twitter and Instagram accounts have been created to promote the positive life of the College. This is controlled by the E-Learning Coordinator and monitored by Senior Leadership.

College staff should ensure that:
- No reference is made in social media to students, parents/ carers or College staff.
- They do not engage in online discussion on personal matters relating to members of the College community.
- Personal opinions are not attributed to the College. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

MANAGING INTERNET ACCESS

INTERNET FILTERING

The College is responsible for ensuring that the College infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections are effective in carrying out their e-safety responsibilities:

- The College will work with C2K, Internet Service Provider to ensure that systems to protect students are reviewed and updated regularly.
- All users have clearly defined access rights to College systems and devices.
- All users are provided with a secure username and password. Users are responsible for the security of their username and password.
- Internet access is filtered for all College users. Content lists are regularly updated and internet use is monitored and logged.
- If staff or students discover an unsuitable site, it must be reported to the C2K Manager/ ICT Technician.

The College will take all reasonable precautions to prevent access to inappropriate material and will review its procedures regularly to ensure protection. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a device connected to the College networks. The College cannot accept liability for any material accessed, or any consequences of internet access.

COLLEGE WEBSITE/ PUBLISHED CONTENT

- Staff or student personal contact information will not be published. The contact details provided on line will be the College office.
- The E-Learning Coordinator will take overall responsibility and ensure that content published is accurate and appropriate.

DIGITAL IMAGES AND VIDEOS

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/ carers and students need to be aware of the risks associated with publishing digital images on the internet. For example, such images could potentially result in cyberbullying. Moreover, digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the 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. on social networking sites.
- Parents/ carers are welcome to take videos and digital images of their children at College events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents/ carers comment on any activities involving other students in the digital/ video images.
- Staff and volunteers are allowed to take digital/ video images to support educational aims, but must follow College policies concerning the sharing, distribution and publication of those images. Those images should only be taken on College equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/ video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of students are published on the College website.

PERSONAL/ CLOUD STORAGE

Students and staff make use of cloud storage operators such as Google Apps for Education or Dropbox. When using this storage the College considers the following as good practice:

- Do not share your username and password.
- Files brought into College on pen drives/ cloud storage must be relevant and appropriate for educational purposes.
- Inappropriate content must be reported to the E-Learning Coordinator immediately.

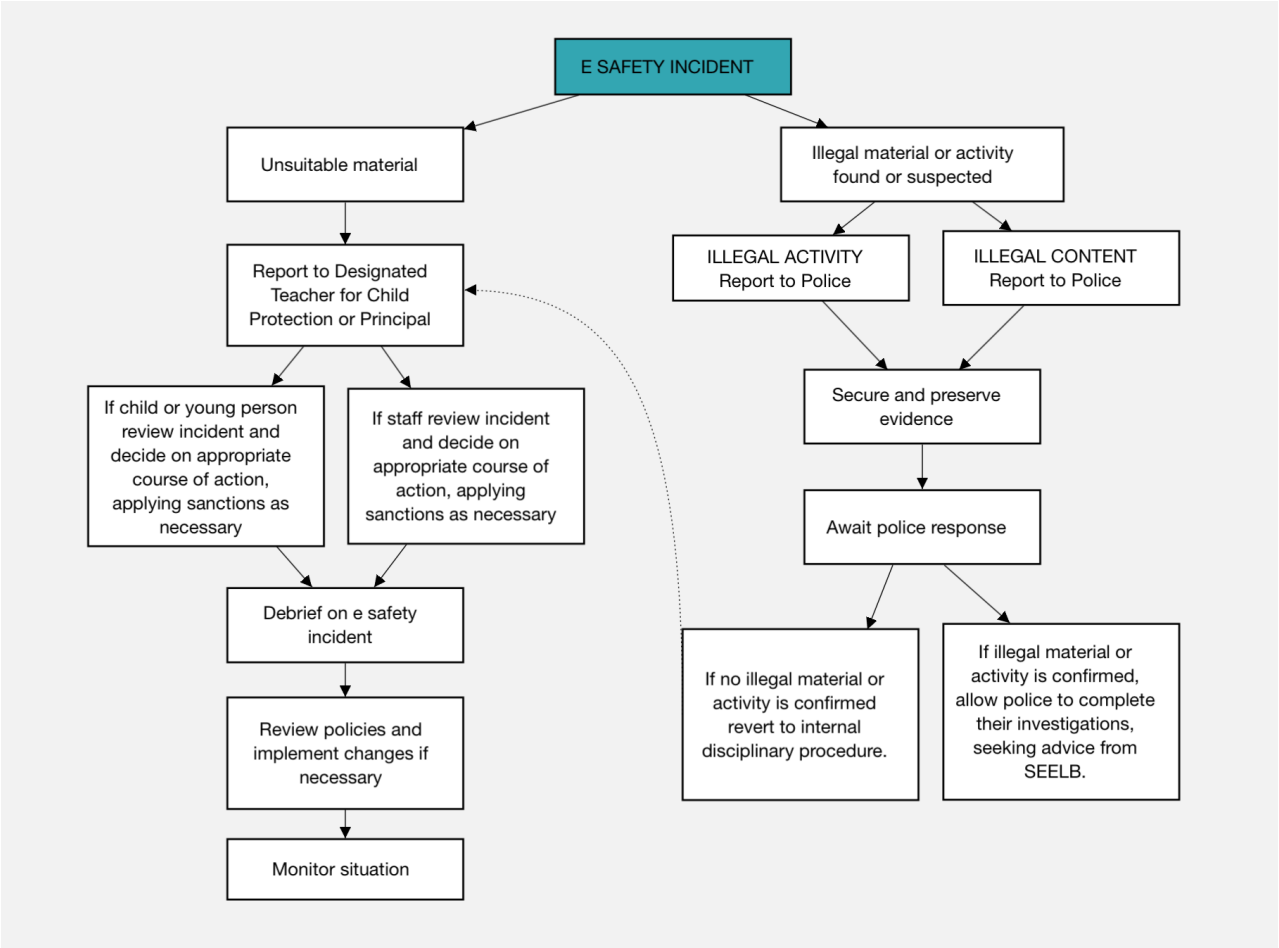
DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR.

RESPONDING TO INCIDENTS OF MISUSE

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Complaints about staff misuse must be referred to the Principal.
- Complaints of a child protection nature with be dealt with by the Designated Teacher in accordance with College child protection procedures.

- Students and parents will be informed of the complaints procedure.



APPENDIX 1 E SAFETY CHARTER - STUDENTS

At Priory College we encourage you to use all of the Information Communication Technology (ICT) available to you – this will help you to enhance your learning. You need to use this technology in a responsible way and make sure that you do not put your own or others' safety at risk.

For my own safety:

- I understand that the College will monitor how I use College ICT systems.
- I will keep my username and password safe and will not use others' log in details.
- I will make sure that I am fully aware of who I am talking to online at all times.
- I will not share personal information about myself or anyone else when online. This includes email addresses, usernames or mobile phone numbers.
- I will tell an adult if I see any inappropriate material or messages online. Or if anything makes me feel uncomfortable.
- I will only open attachments from people I know and will try my best to make sure that there are no viruses on pen drives/ cloud storage that I may use in College.

For my own and others' learning:

- I will respect others' work and property and will not access, copy, remove or change
- someone else's files.
- I will take care while using the College's ICT equipment to prevent it being damaged.
- I will be polite and responsible when communicating with others.
- I will not take or send images of ANYONE without their permission or post photos of students in College uniform to social networking sites.
- I will not "Check In" or refer to Priory College, on social networking sites.
- I will only use my hand held devices (i.e. iPods/ iPads) in College, when I have permission from a teacher.
- I will not install or download programmes to College computers.
- I will not alter computer settings or access blocked websites whilst using the College networks.

I understand that I am responsible for my actions, both in and out of College:

- I understand that College has the right to take action against me if I break these rules or am involved in incidents of inappropriate behaviour, that are covered in this Charter.
- The College may be obliged to report my and/or others' actions to the police if a young person's safety or wellbeing is in danger.
- I understand that I may lose access to the College network if I fail to follow the requirements of this charter.

Please sign below if you understand the above and agree to follow these guidelines when:

- I use the College ICT systems and equipment (both inside and outside of College),
- I use my own equipment in College, or in a way that is related to me being a member of this College community (I.e. using College email or Virtual Learning Environments).

APPENDIX 2 E SAFETY CHARTER - STAFF

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to adhere to this code of conduct. Members of staff should consult the College's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a College ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for College business.
- I understand that my use of College information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in College, taken off the College premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's e-safety to the the Designated Teacher or Principal.
- I will not look at students' profiles on Social Networking Sites to investigate reports of bullying etc. This should be reported to the Head or Year who will pass it onto the relevant authorities.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I understand communication with students, by whatever method, should take place with clear and explicit professional boundaries.
- I will ensure all communications are transparent and open to scrutiny.
- I will not engage, via Social Networks or private email, with any students at Priory Integrated College.
- I will not give personal contact details, including my mobile telephone number, to students or parents.
- I will only use equipment provided by the College to communicate with students.
- I understand I have a duty to protect my password(s), changing them on a regular basis and using strong passwords i.e. a password which contains letters, symbols and
- numbers.
- I understand I should lock the workstation or log off the network when leaving workstations unattended.
- I understand the E-Safety Charter for staff is regularly reviewed and consistently enforced.
- I will maintain high standards of professional conduct in all digital environments.

The College may exercise its right to monitor the use of the College's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the College's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

STAFF USE OF SOCIAL NETWORKING

Many College employees use the web and social networking services such as Facebook, Flickr, YouTube, Instagram and Twitter for work-related projects or for personal use. As a College we acknowledge the significant role social media can play in celebrating the success of our students and raising the profile of the College. Whilst we actively encourage the College community to re-share our social media published content we are also aware of the risks such platforms can offer. While College employees are private individuals, they also have professional reputations and careers to maintain. Additionally, employees are required not to do anything to endanger the health and safety of their colleagues or others.

Managing personal information effectively makes it far less likely that information will be misused. Therefore before you make your next post or tweet – think about:

- When publishing information about yourself or having conversations with others online, be mindful of how you present yourself, who can see your content, and how you manage this appropriately. When publishing information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer, colleague, student or parent, viewing your content.
- Who is allowed to view your content on the sites that you use – and how to restrict access to your account where necessary. If you are not clear about how to restrict access to your content to certain groups of people, regard all of your content as publicly available and act accordingly.

Full guidance and support for staff can be found in our Social Networking and Communication Policy.

YOUTUBE

YouTube is accessible to staff. Remember the following when using it in class:

- Be prepared – search for the appropriate clips prior to your lesson. You should never do this in full view of the class as there is a danger inappropriate content may appear.
- Do not give students access to YouTube from your workstation.
- View content fully before showing it to your class, to ensure it is appropriate.