ST MARY'S HIGH SCHOOL, NEWRY

E-Safety and Internet Acceptable Use Policy

Revised May 2025

Rationale:

As a Rights Respecting School, staff in St Mary's have responsibility for the pastoral care, general welfare and safety of all the students in our school. This duty is carried out in a caring, supportive and safe environment, where each student is valued for her unique talents and abilities, and in which they learn and develop to their full potential. This policy clarifies the responsibilities of staff, students and parents/carers in relation to E-Safety procedures and arrangements.

The E-Safety and Internet Acceptable Use Policy has been written in line with the Department of Education Northern Ireland (DENI) Policy and Guidelines.

Definition:

'E-Safety or electronic safety is about utilising electronic devices or E-technologies in a safe and responsible way. It is mainly concerned with the safeguarding of children and young people in the digital world and educating them so they feel safe when accessing E-technologies.'

(National Children's Bureau NI; 2014)

Article 16: Every child has the right to privacy
Article 17: Every child has the right to reliable information from the mass media
Article 19: Every child has the right to protection

(United Nations Convention for the Rights of the Child)

E-Safety in the school context:

- is concerned with safeguarding all students in the digital world which they now live;
- emphasises using digital technologies in a positive way;
- is concerned with supporting students to develop safer online behaviours both in and out of school;
- is concerned with helping students recognise unsafe situations and how to respond to risks appropriately

Aims:

Effective use of the Internet aims to enrich the learning experience for all students and to ensure that teachers develop confidence and competence to effectively use the Internet as a learning resource to support the teaching of their subject.
The effective use of the Internet offers opportunities to:

- support learning and teaching across the curriculum at all levels;
- enhance and individualise the educational experience, helping students to enjoy learning, improve their performance and raise standards;
- improve standards in literacy, numeracy and attainment in other areas of study;
- elevate student's creativity, developing their digital and visual literacies;

- personalise learning and improve arrangements for assessment for learning, record-keeping and reporting;
- develop the skills needed to be economically active in the global digital economy;
- consolidate the partnership between the school, home and the community;
- develop good health and safety attitudes and practice.

The Importance of Internet Use in Education:

The purpose of Internet use in school is to support Learning and Teaching, to raise educational attainment, to promote student achievement, support the professional work of staff and to enhance the school's management information systems. Through the Preventative Curriculum and Personal Development Programme students will be taught about acceptable and unacceptable use of the Internet.

Supportive and Caring Ethos:

As a Rights Respecting School, the Curriculum and Pastoral Care provisions in St Mary's aims to support all students make responsible decisions in relation to the appropriate safe use of the Internet. These provisions include measures to help meet the physical, emotional and spiritual needs of all learners within an inclusive learning environment.
The Preventative Curriculum and Personal Development Programme allows students to explore key issues within their own personal development including self-awareness, health and well-being, relationships personal safety and managing risks.

Management of E-Safety:

Management of Internet Access:

Parents/Carers give permission for their daughter to use the Internet when in School by signing the Permission Form at the start of the academic year (Appendix 1). If they wish their daughter to use her own Digital Device in school, they must sign the Bring Your Own Device Declaration in their daughter's diary which can be checked by any member of staff.

Management of School e-mail:

Students must use their own approved C2K e-mail accounts and must inform a teacher immediately if they receive offensive e-mail. Students must not reveal details about themselves or others through e-mail communication, such as their address or telephone number. The C2K Education Network filtering system provides security and protection to C2K email accounts. The filtering system offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Management of the School Social Media Content:

Contact details on the school website will only include the school address, school e-mail and telephone number. Staff or students' home information will not be published. Photographs or video that include students will be carefully selected for use on the Website, School App, Facebook or Instagram. Parents/Carers must sign the Permission Form at the start of the academic year before photographs or videos of students are published on school website and social media (Appendix 1). The Digital Technician has sole responsibility for the uploading of content to the school's website/social media accounts. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Social Networking:
St Mary's High School is fully supportive of social networking as a tool to engage and collaborate with learners, and to communicate with parents/carers and the wider school community. The following social media services are permitted for use within St Mary's High School and have been appropriately risk assessed.

- X/Twitter
- Instagram
- TikTok
- Facebook

Should staff wish to use other social media, permission must first be sought via the designated teacher. Any new service will be risk assessed before use is permitted.

Management of Discussion Forums and Video Conferencing:
The use of video conferencing facilities in school will be used for approved educational activities and all such use by students will be monitored by staff members. Students will be allowed to take part in discussion forums that are strictly controlled by staff or other responsible adults within and outside school using approved online learning environments, e.g. Collaborate Ultra. (no longer used, as far as I know)

External Access to User Areas and Learning Environments:
The school will grant students and staff access to their user areas on online learning platforms from home. The school is not liable for any loss or damage to students or staff files caused unintentionally or by inappropriate or misguided use of the facilities.

Management of Wireless System and Emerging Technologies:
The Digital Technologies related Policies will be reviewed on an annual basis to take account of the risks associated with emerging technologies. The school has wireless coverage throughout the building hence additional associated risks are possible. **Annually, parents/carers acknowledge their acceptance of the school's Digital Technology/IT Rules by signing the school rules in their daughter's diary. These rules state that mobile phones must be switched off during the school day between the hours of 9:00am and 3:00pm. This includes the use of any mobile technology to access the Internet through the school's wireless network. Use of mobile phones in a lesson can only take place with the permission of the classroom teacher.**

Portable storage devices such as MP3 players, are these used nowadays? PDAs, Camera Phones, or any other device that is capable of storing and displaying images or video, should not be used between the 9:00am and 3:00pm unless it is for educational purposes and in the presence of the class teacher.

Students and staff are allowed to use portable storage devices such as flash drives or memory sticks, however these must be checked for viruses prior to use. Neither students nor staff will be allowed to install applications of any type from portable storage devices without gaining permission from the Digital Technician (Miss Doyle).

All students must comply with the E-Safety and Internet Acceptable Use Policy. Parents/Carers are asked at the start of each academic year to read the Bring You Own Device Policy on the school app and sign the declaration statement to acknowledge their consent.

Management of Risk Assessment:
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. Students need to become 'Internet-wise' and ultimately good 'digital citizens'. Students need to know what to do if they come across inappropriate material or situations online. These risks have been defined and categorised by the NCB NI as follows:

- *Content Risks: The young person is exposed to harmful material;*
- *Contact Risks: The young person participates in adult initiated online activity;*
- *Conduct Risks: The young person is a perpetrator or victim in peer-to-peer exchange;*
- *Commercial Risks: The young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs*

However, due to the international scale and linked nature of internet content and while all the necessary safeguarding procedures and policies are in place, it is not possible to guarantee that unsuitable material will never appear on a school computer. **The school cannot accept liability for the material accessed, or any consequences of Internet access.**

Management of Acceptable Online Content:
If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Digital Technician (Miss Doyle) or the Vice Principal who will report the URL to C2K. The school should ensure that the use of Internet derived materials by staff and by students complies with copyright law. The school will inform all staff and students of the appropriate way to use copyright material legally in school.

Fair Processing Notice:
Students, as part of their education in St Mary's High School will have access to a range of electronic resources designed to enhance their learning experience and allow them to collaborate with their peers. In order to facilitate this, the School may need to share some limited personal information with the Education Authority, Department of Education and Examination Bodies. This will allow user accounts to be set-up and managed, enabling services to be integrated. Any data sharing is kept to a minimum and when your child leaves the School the information will be permanently deleted from such systems. At times, the School may also share personal information with the Education Authority to support the direct delivery of educational services, including Special Education and Educational Psychology Services, Social Services, CLA Team, Department of Education, Education Authority, Education Welfare Service, Behaviour Support Team and the PSNI. All sharing will be conducted under the provisions of the Data Protection Act 2018'.

E-Safety Initiatives in St Mary's:
Young people's extensive use of digital technologies means staff need to be able to take appropriate preventative actions to minimise the associated risks. The following initiatives are established in St Mary's:

- St Mary's is a Rights Respecting School where all students feel valued, safe, respected and supported;
- Through our Pastoral Programme we offer a supportive and caring environment to all students. The Preventative Curriculum and Personal Development Programme allows students to explore key issues within their personal development including Self Concepts, Self Esteem, Health and Well-being, Relationships and Personal Safety; (change as previously perhaps?)
- **E-Safety Lessons:**

Year	Theme
8	Cyberbullying Sharing Information Online PSNI Talk – Online Safety
9	Staying Safe Online PSNI Talk – Cyberbullying
10	Meeting Strangers Online PSNI Talk -Sextortion
11	My Online Reputation
12	Sending Images Online

- The school uses a range of external agencies for E-Safety support and guidance including PSNI, EA CPSS, Education and Welfare Office, Student Personal Development Service, Behaviour Support Team, School Counsellor;
- The E-Safety Code is displayed throughout the school and referred to on a regular basis (***Appendix 2)***
- Whole staff training;
- The Child Protection Policy is reviewed on an annual basis and available on the School App and Website.
- The Staff Code of Conduct is shared with all adults working in school;
- All staff and volunteers receive Child Protection Training;
- The Safeguarding Team Poster is displayed in every classroom and on the Safeguarding Noticeboard;
- Digital Learning Ambassadors promote E-Safety messages through social media and morning assemblies;
- Students are regularly reminded of the Designated and Deputy Designated Teachers;
- Lunchtime supervision is provided by non-teaching members of staff who have received full Child Protection training;
- All new staff and volunteers are fully vetted prior to commencement of employment in school

Staff and students at St. Mary's High School should **know and understand** that no Digital Technology user is permitted to:

- retrieve, send, copy or display offensive messages or pictures;
- use obscene or racist language;
- harass, insult or attack others;

- damage computers, computer systems or computer networks;
- damage any digital equipment in school;
- violate copyright laws;
- use another user's password;
- access another user's folders, work or files;
- intentionally waste resources such as paper or ink;
- use the network for unapproved commercial purposes;
- access inappropriate or unacceptable sites.

If the school feels that a student has brought its reputation into disrepute by publishing unsuitable comments or images about other students or members of staff, or through publishing unsuitable materials that may appear to be linked to the school or identify the school in any unfavourable way, then these matters will be investigated and suitable sanctions imposed. In extreme cases the social networking site in question, or the PSNI, will be contacted to have the material in question removed. In such cases where the student is found to have broken the schools code of conduct, this will be considered serious misconduct and will dealt with appropriately which may lead to suspension or expulsion.

Cyber Bullying:

Developments in Digital Technologies have made instances of cyber bullying more widespread. ***Research findings from the NSPCC (2023) show that 19.1% of children aged 10 to 15 experienced online cyber bullying.***

Some examples of cyber bullying include:

- Text messages that are threatening or upsetting;
- Offensive posts online;
- Still images and video clips captured on and circulated by mobile phones to cause embarrassment to the student, who may not even know that they have been photographed or videoed in line with e safety policy;
- Threatening emails, often using a fictitious name or someone else's name;
- Anonymous calls or abusive messages to another mobile phone – sometimes the person who is being bullied has her phone stolen and it is used to harass others, who then think the owner of the phone is responsible.
- Sexting can also occur where someone is encouraged to share intimate pictures or videos of themselves and these are then transmitted to other people;
- Instant Messaging (IM) conveying threats or insults in real-time conversations;
- Defamatory messages broadcast on Websites, Blogs, Twitter, Personal or Social Networking Sites (Eg. Facebook, Instagram, Snapchat);
- Menacing or upsetting responses in Chat Rooms;
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.

Whilst cyber-bullying may appear to provide anonymity, most messages can be tracked back to the creator and students are reminded that cyber-bullying can constitute a criminal offence. As with conventional forms of bullying, many children do not tell anyone they are experiencing bullying type behaviour by another person via the Internet or mobile phone. It is imperative that the student informs a parent/carer or member of staff if they are experiencing bullying type behaviour through technologies such as mobile phones or the Internet.

- If the alleged electronic bullying type behaviour has an impact on relationships between pupils in school, staff will investigate the incident providing support to both the pupil experiencing and the pupil displaying bullying type behaviour.
- It is the policy that staff will not look through a students' mobile phone or read information or look at photos on a student's social networking site.
- The Vice Principal and the Principal together may request a student to allow them to view evidence of a socially unacceptable or potentially bullying type behaviour contained on electronic devices. The student's parents/carers will be notified before this request is made and informed of the outcome.
- If a student refuses to share the electronic evidence with the Principal and Vice Principal their parents/carers will be requested to come into the school immediately.
- Evidence may be shared with the PSNI to aid investigations of child protection or potentially law-breaking behaviour.

School Responsibilities:

- To promote an ethos of respect for self, for others and the environment;
- To set the highest possible standards for positive relationships among staff, students and parents/carers;
- To ensure a safe e-learning environment for staff and students;
- To encourage openness about any form of unacceptable bullying type behaviour in relation to the Internet;
- To investigate any reports of bullying type behaviour;
- To seek advice from the PSNI if the school has been informed that a student under the age of 16 shares an indecent picture through Social Media (E.g., Instagram or Snapchat);
- To take appropriate action when alleged cyber bullying type behaviour is reported;
- To involve parents/carers in addressing a problem situation when necessary;
- To promote the need for respectful behaviour, rights and responsibilities through the Pastoral Care and Personal Development Programmes and assemblies;
- To support and help both the student experiencing bullying type behaviour and the student displaying bullying type behaviour;
- To provide E-Safety and Child Protection training for all members of staff.

Parent/Carer Responsibilities:

- To promote respect for self, others and property and support the school rules;
- To discuss with their daughters any fears or experiences of what appears to be bullying type behaviour;
- To help their daughter's work out simple, non-aggressive, strategies for dealing with what appears to be worrying behaviour on the part of another person;
- To discourage any tendency towards bullying type behaviour on the part of their daughter;
- To support the school procedures for dealing with alleged bullying type behaviour as outlined in the Anti Bullying Policy;
- To inform the school of any serious concern regarding alleged cyber bullying type behaviour;
- To co-operate with the school in resolving any difficulties involving alleged bullying type behaviour;
- To seek advice from the PSNI if they know their daughter is experiencing bullying type behaviour outside the school environment via social networking sites, mobile phones or the internet;
- To inform the PSNI if it is known that a young person under the age of 16 shares an indecent picture through Social Media (E.g., Instagram or Snapchat);

- To resolve situations/difficulties outside of school which may impact on behaviours of students in school.

Student Responsibilities:

- To respect herself, others and the environment;
- To know her rights and responsibilities regarding personal safety;
- To have confidence in staff and to report any concerns regarding alleged bullying type behaviour, whether for her own safety or the safety of others;
- To tell her parents/carers if she is experiencing bullying type behaviour;
- To practice self-control and avoid reacting to negative attitudes or behaviours of others in an aggressive way and to report such incidents to a member of staff;
- To avoid engaging in any forms of cyberbullying that may cause distress to others;
- To be aware of the consequences of cyberbullying.

Advice to Parents/Carers on use of e-Media and Social Networking Sites:

St. Mary's implements a **filtered** Internet and e-mail service. During school hours teachers will guide students towards appropriate materials on the Internet. However, it is at all times the student's responsibility to ensure that only appropriate material is accessed.

Outside school, parents/carers bear the same responsibility for such guidance as they would normally exercise with other multimedia information sources. **Parents/Carers should be aware that they are responsible for their daughter's supervised use of the Internet at home.** The aim of this policy is to help parents/carers understand online safety issues and give practical advice on the Internet using SMART safety tips. While it is fair to say that many children may have better technical skills than their parents/carers, they still need parental advice and protection when using the Internet.

The school aims to educate parents/carers and students of the dangers associated with social networking sites by offering support through the delivery of the curriculum and information shared through the School App or other forms.

Discussing possible dangers needs care and sensitivity. The following **SMART** TIPS have been written especially for children aged 8 – 16 years.

S	Secret	Keep personal information such as name and address private.
M	Meeting	Never meet anyone unsupervised by an adult.
A	Accepting	Never accept e-mails from people you don't know, they may contain a virus or nasty message.
R	Remember	Someone online may be lying and not be who they say they are.
T	Tell	Tell your parent/carer or a trusted adult if someone or something online makes you uncomfortable or worried

***Advice and guidance includes the following*:**

- Parents/carers should discuss with their children the rules for using the Internet and decide together when, how long, and what comprises appropriate use;
- Parents/carers should discuss with their children the appropriate use of Social Networking Sites such as Facebook; Snapchat, Instagram, Twitter, TikTok, etc. Cyberbullying is a serious offence and therefore the PSNI will become involved if the school or parents/carers feel that it is in the best interests of the child to make a referral;

- Parents/carers should get to know the sites their daughter/s visit, and discuss what they are learning;
- Parents/carers should ensure they protect their daughter from unwanted or unacceptable overtures from strangers and encouraging them to keep personal identifying information private;
- Parents/carers should encourage their daughter to never respond to any unwelcome, unpleasant or abusive messages and to tell a responsible adult if they receive any such messages or images. If a message comes from the C2K Internet Service connection provided in school, they should immediately inform the Vice Principal (Designated Teacher) or Principal.

Sanctions

- Violation of the rules for the appropriate use of Digital Technology in school shall result in a temporary or permanent ban on the use of the network;
- Parents/carers will be informed;
- Disciplinary action will be taken in line with existing school policy on inappropriate behaviour;
- Where applicable, the PSNI or local authorities may be involved.

Management of Printing Credits:

The school operates a 'Printing Credits' system in which all students are allotted an adequate number of printing credits for each term, reviewed on an annual basis. This system has been put in place to help dissuade students from needlessly printing work or from printing materials of a non-educational basis. The school endeavours to make students aware of the costs associated with printers and it is the responsibility of students to ensure that they have enough printing credits available to print their schoolwork in advance of any coursework/ homework deadline. If students exceed their printer credit allocation they can purchase additional credits from the Digital Technology Technician. Students should not allow others to use their print credits to print their work. Students will not be allowed extra credits if disputes arise concerning the misuse of the printing credits system, this includes accidental or unintentional use.

Informing Students about the e Safety and Internet Acceptable Use Policy:

Parents must provide written permission for their daughter to be given restricted access to the Internet in school at the beginning of each school academic year (Appendix 1). Students must also agree to the acceptable use of Internet access at the beginning of each school academic year. Rules for acceptable use are included in student's homework diary. Students will be informed that Internet use will be monitored and security reports are accessed. Guidance in responsible and safe use will precede Internet access.

Management of Complaints Regarding the Internet:

Responsibility for handling incidents will be delegated to the Digital Technician and/or Vice Principal. Any complaint about student or staff misuse must be referred to the Principal.

E-Safety Agencies:

- PSNI – Police Service Northern Ireland – delivers Internet safety programmes
- Child Exploitation and Online Protection (CEOP): www.thinkuknow.co.uk – CEOP is part of the UK policing structures and its key functions include tracking and bringing offenders to account either directly or in cooperation with local and international police forces and work with children, parents/carers and practitioners to deliver the Thinkuknow Internet Safety Programme

- C2K – Northern Ireland Schools managed computer system – E-Safety support for all teachers in Northern Ireland
- NSPCC – staff are trained as CEOP ambassadors to deliver the CEOP Thinkuknow programme
- Northern Ireland Anti Bullying Forum (NIABF) – focuses on cyberbullying
- External Speakers – PSNI – E-Safety presentations to staff and (take out?) students.

Consultation:

During the review of this document consultation took place with the following groups:
Students – through the Rights Respecting Council
Parents/Carers – through the Parent Teachers Friends Association
Staff
Board of Governors

Related School Policies:

This policy is set within the broader school context of Pastoral Care and as such should be implemented in conjunction with the following school policies:

- Digital Learning Policy
- Child Protection Policy
- Anti Bullying Policy
- BYOD Policy
- RSE Policy
- Positive Behaviour Policy
- Staff Acceptable Use Policy

Dissemination of the e Safety Policy:

A summary of key Pastoral Policies are given to all parents/carers of new students and are available on the School App and Website. An overview of the policies is sent to all parents at the start of each academic year.

Monitoring, Evaluation and Review

The Vice Principal and Designated Teacher, Mr Fitzpatrick is responsible for monitoring, evaluating and reviewing the implementation of the E-Safety and Internet Acceptable Use Policy to ensure:

- the effective implementation of this policy;
- that the policy is updated in the light of new developments in Digital Technologies;
- the implementation of the policy is reviewed and advise the Principal and SLT on a regular basis.

Signed by Chair of Governors: _____

Date: _____

Signed by Principal: _____

Date: _____

Date of Review: __May 2028_____

Appendix 1

PERMISSION FORMS

Student Name: _____ Form Class:

Use of School Internet

I understand that access to the Internet in St Mary's High School is for educational purposes only. Access is given to students who act in a considerable and responsible manner and should be withdrawn if they fail to maintain acceptable standards of use. I accept that the school is not responsible for any unsuitable materials acquired from the Internet by my daughter and will ensure she does not bring unsuitable material into the school.

Signed: _____ **Signed:** _____

(*Student)* ***(Parent/Carer)***

Use of your Daughter's Photograph

To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain consent to use a student's image for example in school displays, local press, newsletters, prospectus and our social media platforms. We would appreciate it if you would give permission for your daughter's photograph to be used for these purposes.

I agree that the school can use my daughter's photograph for the purposes mentioned above.

Signed: _____ ***Date:*** _____

(Parent/Carer)

Sharing Personal Information with Careers Service *(Years 10-14 only)*

On occasions the school is asked to share basic personal information with the Careers Service to allow them to provide advice and guidance to students. To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain express consent for the use of your child's personal information for use by the Careers Service. On occasions the careers service may need to contact students when at home.

I agree that the school can share basic information with the Careers Services for the purposes mentioned above and for advisers to contact my daughter at home.

Signed: _____ ***Date:*** _____

(Parent/Carer)

Online Activities/Using Mobile Phone

Students may be involved in online learning that may include participating in online activities through platforms including: Zoom, Collaborate, Google Meet, Teams or any other software package and may require students using their mobile phone. Students are not allowed to record, store or transmit any type of personal image or sound of any other student or adult except for approved educational tasks. This means that taking pictures or filming in school, even of friends, is not allowed except when approved is given from the class teacher. If you give your daughter permission to participate in the online discussion and activity, please sign the form below.

Signed: _____ ***Date:*** _____

(Parent/Carer)

Appendix 2

E Safety Code

My Digital Footprint

To have a good online reputation

- Stop and think about what you send
- Never send or upload something you may later regret
- Never give information about yourself online
- Remember everything sent can be retrieved
- Remember employers and universities will check you out

UNCRC Article 16 Right to

S T A M P