ST MARY'S HIGH SCHOOL, NEWRY

E Safety and Internet Acceptable Use Policy

Revised June 2019

Rationale:

As a Rights Respecting School, staff in St Mary's have a responsibility for the Pastoral Care, general welfare and safety of the children in our care and we will carry out this duty by providing a caring, supportive and safe environment, where each child is valued for her unique talents and abilities, and in which all our young people can learn and develop to their full potential. This policy clarifies the responsibilities of staff, parents and pupils 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. It has been agreed by staff and pupils and ratified by the Board of Governors and will be reviewed every two years.

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 children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school;
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately

Aims:

The overall aim for the effective use of the Internet is to enrich the learning for all pupils and to ensure that teachers develop confidence and competence to use the Internet as a additional 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 their educational experience, helping them to enjoy learning, improve their performance and raise standards;

- improve their standards in literacy, numeracy and other areas of study;
- meet the requirements of the Northern Ireland Curriculum for assessing and reporting the cross curricular skill 'Using ICT';
- elevate pupil's creativity, developing their digital and visual literacies;
- personalise learning and improve arrangements for assessment for learning, record-keeping and reporting;
- use an appropriate blend of non-technological and online methods of learning, connecting to other learners through online networks;
- develop the skills needed to be economically active in the global knowledge 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:

For most young people e-technology is part of everyday life and this has become even more apparent in the current research NCB NI is conducting on behalf of OFMDFM where findings show, for example, that four out of five young people (79%) go online everyday and in excess of one in five young people (22%) spend five hours or more online everyday. Pupils spend 8 hours 41 minutes on electronic devices a day (average pupils sleep 8 hours 21 minutes). The purpose of Internet use in school is to support Learning and Teaching, to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Pupils will learn digital literacy skills and refine their own publishing and communications with others via the Internet. Through the Personal Development Programme pupils will be taught about acceptable and unacceptable use of the Internet.

Supportive and Caring Ethos in School:

As a Rights Respecting School, the Curriculum and Pastoral Care provisions in St Mary's aim to help and support all pupils 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 Personal Development Programme allows pupils to explore key issues within their personal development including self concepts, esteem, health and well-being, relationships and personal safety.

Management of e Safety in St Mary's:

Management of Internet Access:

Parents must provide written permission for their daughter to be given restricted access to the Internet in school. Pupils must apply for Internet access individually by agreeing to the acceptable use of the e Safety and Internet Acceptable Use Policy.

Management of School e-mail:

Pupils must use their own approved C2K e-mail accounts and must inform a teacher immediately if they receive offensive e-mail. Pupils must not reveal details about themselves or others through e-mail communication, such as their address or telephone number. The C2K Education Network filtering solution provides security and protection to C2K email accounts. The filtering solution 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 Website Content:
Contact details on the website will only include the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Photographs or video that include pupils will be carefully selected for use on the Website, School App, Facebook or Twitter. Parents must sign a consent form before photographs or videos of pupils are published on the school website. The ICT Technician has sole responsibility for the uploading of content to the website. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Social Networking:
There are many social networking services available; St Mary's High School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents 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; should staff wish to use other social media, permission must first be sought via designated teacher. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school.
- Twitter – used by the school as a broadcast service (see below)
- Facebook – used by the school as a broadcast service (see below)

A broadcast service is a one-way communication method in order to share school information with the wider school community.

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 pupils will be monitored by staff members. Pupils 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. the school's FRONTER.

External Access to User Areas and Learning Environments:
The school will grant pupils and staff access to their user areas or FRONTER from home using their own username and password. The school is not liable for any loss or damage to pupils or staff files caused unintentionally or by inappropriate or misguided use of the facilities.

Management of Wireless System and Emerging Technologies:
The ICT 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 sign up to the agreed school rules which 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 or World Wide Web through the school's wireless network.**

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment may need to be undertaken on each new technology for effective and safe practice in classroom use. New applications are continually being

developed based on the Internet, mobile phone network, wireless, Bluetooth or infrared connections.

Portable storage devices such as MP3 players, 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.

Pupils 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 pupils nor staff will be allowed to install applications of any type from portable storage devices without gaining permission of the C2K Manager or ICT Technician (Miss Doyle).

Pupils and staff will only be allowed to use personal laptops or PDA's within the school if they seek permission from the C2K Manager. Appropriate virus protection software must be installed on the device. (*BYOD Policy)*

Management of Risk Assessment:
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. Pupils need to become 'Internet-wise' and ultimately good 'digital citizens'. Pupils need to know how to cope 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 pupils discover unsuitable sites, the URL (address) and content must be reported to the C2K Manager or ICT Technician (Miss Doyle) who will report the URL to C2K. The school should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. The school will inform all staff and pupils of the appropriate way to use copyright material legally in school.

Fair Processing Notice:
'Pupils, as part of their education at 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 relevant Education Authority and the Department of Education. 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. Examples include the Authority's Special Education and Educational Psychology Services, Social Services, LAC Team, Department of Education, Education Authority, Education Welfare Service, Behaviour Support Team. All sharing will be conducted under the provisions of the Data Protection Act 1998'.

E Safety Initiatives in St Mary's:
Young people's extensive use of e-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 and Welcoming School where all pupils feel valued, safe, respected and supported;
- Through our Pastoral Programme we offer a supportive and caring environment to all pupils. The Personal Development Programme allows pupils to explore key issues within their personal development including Self Concepts, Self Esteem, Health and Well-being, Relationships and Personal Safety;
- **e Safety Lessons:**

Year	Theme
8	Cyberbullying Sharing Information Online PSNI Talk – Online Safety
9	Staying Safe Online PSNI Talk – Sending Images Online
10	Meeting Strangers Online
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 e Safety Advisers, Education and Welfare Office, Pupil Personal Development Service, Behaviour Support Team, Newry Adolescent Partnership, CAMs, CAPS, Just Ask, School Counsellor;
- PSNI and EA's Safety Support Programmes;
- The e Safety Code is displayed throughout the school and referred to on a regular basis (***Appendix 1)***
- Acceptable 'Use of School Internet' permission slip is signed by pupils and parents before pupils are given access rights to the internet annually;
- Whole staff and Parents e Safety Seminars;
- The Child Protection, ICT, e safety and Internet Policies are reviewed on an annual basis and shared with Governors, Staff, Parents and Pupils;
- The Staff Code of Conduct is shared with all adults working in school;
- All staff and volunteers receive Child Protection Training;
- A Safeguarding Team Poster is displayed in every classroom;
- ICT Ambassadors promote e Safety messages through social media and morning assemblies;
- The Safeguarding Team photos are displayed on a notice board in school;
- Pupils 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 pupils at St. Mary's High School should **know and understand** that no ICT 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 other ICT equipment in school;
- violate copyright laws;
- use another user's password;
- access another user's folders, work or files;
- intentionally waste ICT resources such as paper or ink;
- use the network for unapproved commercial purposes;
- access inappropriate or unacceptable sites.

If the school feels that a pupil has brought its reputation into disrepute by publishing unsuitable comments or images about other pupils 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 pupil 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 Information and Communication Technology (ICT) have made instances of cyber bullying more widespread. ***Research findings from the NSPCC (2013) show that one in five children had been targets of cyber bullying in the last year and 10% of 11 to 16 year olds have been targeted by Internet 'trolls'.*** 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 pupil, 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 for the bully, most messages can be tracked back to the creator and pupils are reminded that cyber-bullying can constitute a criminal offence. As with many conventional forms of bullying, many children do not tell anyone they are being bullied by another person via the Internet or

mobile phone. It is imperative that the pupil informs a parent/guardian or member of staff if they are being bullied through technologies such as mobile phones or the Internet.

It is the Policy in St Mary's for staff <u>not</u> to look through a pupil's mobile phone or read information or look at photos on a pupil's social networking site. If a parent/guardian discovers that their daughter is being bullied via the internet or mobile phone, the school advises that they should seek advice from the PSNI. If the bullying has an impact on the behaviours or relationships between pupils in school, staff will investigate the incident in line with the Behaviour Policy and procedures.

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, pupils and parents;
- To ensure a safe e learning environment for staff and pupils;
- To encourage openness about any form of unacceptable bullying behaviour in relation to the Internet;
- To investigate any reports of cyber bullying if it has an impact on behaviours or relationships between pupils in school;
- To seek advice from the PSNI if the school has been informed that a pupil under the age of 16 shares an indecent picture through Social Media (Eg. Instagram or Snapchat);
- To take appropriate action when cyber bullying is reported;
- To involve parents in addressing a problem situation when necessary;
- To promote the need for respectful behaviour, rights and responsibilities through the Pastoral and Personal Development Programmes and assemblies;
- To encourage the development of resilience among pupils when faced with diversity;
- To support and help both the person being bullied and the person bullying;
- To provide e Safety and Child Protection training for all members of staff.

Parent Responsibilities:

- To encourage their daughter to have self-confidence and to have confidence in talking to staff;
- 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 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 behaviour on the part of their daughter;
- To encourage their daughter to accept the right of staff to correct them for poor behaviour;
- To inform the school of any serious concern regarding cyber bullying behaviour;
- To co-operate with the school in resolving any difficulties involving bullying;
- To seek advice from the PSNI if they know their daughter is being bullied 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 (Eg. Instagram or Snapchat);
- To resolve situations/difficulties outside of school which may impact on behaviours of pupils in school.

Pupil 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 bullying whether for her own safety or the safety of others;
- To tell her parents/guardians if she is being bullied;
- 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 cyber bulling that may cause distress to others;
- To be aware of the consequences of cyber bullying.

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

St. Mary's implements a **filtered** Internet and e-mail service through the C2K system. During school hours teachers will guide pupils towards appropriate materials on the Internet. However, it is at all times the pupil's responsibility to ensure that only appropriate material is accessed.

Outside school, parents or guardians bear the same responsibility for such guidance as they would normally exercise with other multi media information sources. **Parents should be aware that they are responsible for their children's supervised use of the Internet at home.** The aim of this policy is to help parents/guardians 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, they still need parental advice and protection when using the Internet.

The school will aim to educate parents/guardians and pupils of the dangers associated with social networking sites by offering support through the delivery of the curriculum and information shared at Parent Teacher Meetings, Seminars and through ICT related policies.

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/guardian if someone or something makes you uncomfortable or worried

***Our advice and guidance includes the following*:**

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

- Parents should ensure they protect their children from unwanted or unacceptable overtures from strangers and encouraging their children to keep personal identifying information private;
- Parents should encourage their children never to 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 ICT in school shall result in a temporary or permanent ban on the use of the network;
- Parents/guardians 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 pupils 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 pupils from needlessly printing work or from printing materials of a non-educational basis. The school endeavours to make pupils aware of the costs associated with printers and it is the responsibility of pupils to ensure that they have enough printing credits available to print their school work in advance of any coursework/ homework deadline. If pupils exceed their printer credit allocation they can purchase additional credits from the ICT Technician. Pupils should not allow others to use their print credits to print their work. Pupils will not be allowed extra credits if disputes arise concerning the misuse of the printing credits system. This includes accidental or unintentional use.

Informing Pupils 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. Pupils 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 pupil's homework diary. Pupils will be informed that Internet use will be monitored and security reports are accessed by the Principal. Guidance in responsible and safe use will precede Internet access.

Management of the ICT System Security:

The school ICT system will be reviewed regularly in relation to security. Virus protection will be installed and updated regularly. Security strategies will be discussed with C2K, particularly in regards to the Wide Area Network. If a member of the technical support staff leaves then all administrator level usernames and passwords will be changed.

Management of Complaints Regarding the Internet:

Responsibility for handling incidents will be delegated to the C2K Manager. Any complaint about pupil or staff misuse must be referred to the Principal.

E Safety Agencies:

- PSNI – Police Service Northern Ireland – delivers Internet safety programme
- 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 cyber bullying
- Beat the Cyber Bully – delivers workshops
- External Speakers – Mr Wayne Denner – e Safety presentations to staff and pupils.

Related School Policies:

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

- ICT Policy
- Child Protection Policy
- Anti Bullying Policy
- BYOD Policy
- Internet Policy
- RSE Policy
- Behaviour Policy
- Staff Acceptable Use Policy

Dissemination of the e Safety Policy:

Pastoral Policies are given to all Year 8 parents and are available on the school's 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 ICT technologies;
- the implementation of the policy is reviewed and advise the Principal and SLT on a regular basis.

Appendix 1

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