St. Mary's Grammar School, Belfast

ONLINE SAFETY POLICY

December 2017

Online Safety Policy Statements

Education – students

The education of students in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

➢ A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

➢ Key e-safety messages should be reinforced as part of a planned programme of assemblies.

➢ 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 helped to understand the need for an Acceptable Use Policy and encouraged to adopt safe and responsible use of tablets both within and outside school.

➢ Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

➢ Rules for use of tablets will be posted in all rooms and displayed on log-on screens.

➢ Staff should act as good role models in their use of ICT, the internet and tablets.

Education – 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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.
The school will therefore seek to provide information and awareness to parents and carers through:

➢ Letters

➢ School web site

➢ Parental induction evenings

➢ Parental meetings

Education & Training – 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.

➢ 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 school e-safety policy and Acceptable Use Policies.

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

➢ The schools ICT Coordinator will provide advice / guidance / training as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered through participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

➢ There will be regular reviews and audits of the safety and security of school ICT systems.
➢ Servers, wireless systems and cabling must be securely located and physical access restricted.
➢ All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by schools ICT Coordinator and will be annually reviewed.
➢ All users will be provided with a username and password by (Mr Stephen Smart) who will keep an up to date record of users and their usernames. Users will be required to change their password twice a year.
➢ The passwords for the school WIFI system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior teacher and kept in a secure place (eg school safe)

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Samsung.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal (or other nominated senior teacher).
- Any filtering issues should be reported immediately to Samsung.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place (to be described) for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, tablets from accidental or malicious attempts which might threaten the security of the school systems and data.
- Standard temporary access will be available for "guests" (eg sub teachers, visitors) onto the school system.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students community users) and their family members are allowed on tablets that may be used out of school.
- An agreed policy is in place (to be described) that allows staff to / forbids staff from installing programmes on school tablets.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- ➢ During 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, eg using search engines, staff should be vigilant in monitoring the content of the websites they visit.
- ➢ It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- ➢ Fairly and lawfully processed
- ➢ Processed for limited purposes
- ➢ Adequate, relevant and not excessive
- ➢ Accurate
- ➢ Kept no longer than is necessary
- ➢ Processed in accordance with the data subject's rights
- ➢ Secure
- ➢ Only transferred to others with adequate protection.

Staff must ensure that they:

- ➢ At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- ➢ Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- ➢ Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- ➢ Data must be encrypted and password protected.
- ➢ The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- ➢ The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of tablets in social time	✔					✔		
Taking photos on tablets or other camera devices	✔						✔	
Use of personal email addresses in school, or on school network	✔							✔
Use of school email for personal emails	✔						✔	
Use of chat rooms / facilities				✔				✔
Use of social networking sites				✔				✔
Use of blogs		✔					✔	

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

➢ The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
➢ Users need to be aware that email communications may be monitored
➢ Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
➢ Any digital communication between staff and students or parents / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
➢ Whole class or group texting will be used at all key stages.

> Personal information should not be posted on the school website/facebook page/twitter page and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions: **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:**	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
child sexual abuse images					✓
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
adult material that potentially breaches the Obscene Publications Act in the UK					✓
pornography				✓	
promotion of any kind of discrimination or racial/religious hatred				✓	
threatening behaviour, including promotion of physical violence or mental harm				✓	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business			✓		
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school			✓		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions			✓		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)			✓		
Creating or propagating computer viruses or other harmful files			✓		
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet			✓		
Use of social networking sites				✓	

Responding to incidents of misuse

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Incidents: Students	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓			✓	✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓				✓	✓		✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓			✓
Unauthorised downloading or uploading of files	✓	✓			✓	✓			✓
Allowing others to access school network by sharing username and passwords or using the account of a member of staff	✓				✓	✓	✓	✓	
Corrupting or destroying the data of other users		✓			✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓	✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓			✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓	✓	✓	✓	✓

Incidents: Staff	Actions / Sanctions							
	Refer to line manager	Refer to Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).								
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or accessing the school network, using another person's account								
Careless use of personal data eg holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's filtering system								
Accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								

Student Acceptable Use Policy Agreement Template

School Policy

New 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 digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

> ➢ that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
> ➢ that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

> ➢ I understand that the school will monitor my use of the ICT systems, email and other digital communications.
> ➢ I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
> ➢ I will be aware of "stranger danger", when I am communicating on-line.
> ➢ I will not disclose or share personal information about myself or others when on-line.
> ➢ If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
> ➢ I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

➢ I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
➢ I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
➢ I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

➢ I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
➢ I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
➢ I will not take or distribute images of anyone without their permission.

I recognize that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

➢ I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
➢ I will immediately report any damage or faults involving equipment or software, however this may have happened.
➢ I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
➢ I will not install or attempt to install programmes of any type on a machine, or store programmes on a tablet, nor will I try to alter tablet settings.
➢ I will only use chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognize that:

➢ I should ensure that I have permission to use the original work of others in my own work
➢ Where work is protected by copyright, I will not try to download copies (including music and videos)
➢ When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

➢ I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

➢ I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Policy (AUP), to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

➢ I use the school ICT systems and equipment (both in and out of school)

➢ I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Group / Class	

Signed		Date	

Staff Acceptable Use Policy Agreement Template

School Policy

New 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 digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

> ➢ that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
> ➢ that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
> ➢ that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

> ➢ I understand that the school will monitor my use of the ICT systems, email and other digital communications.
> ➢ I understand that the rules set out in this agreement also apply to use of school ICT systems (eg tablets, laptops, email, VLE etc) out of school.
> ➢ I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
> ➢ I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
> ➢ I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- ➢ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- ➢ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- ➢ I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- ➢ I will only use chat and social networking sites in school in accordance with the school's policies.
- ➢ I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- ➢ I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- ➢ When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- ➢ I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- ➢ I will ensure that my data is regularly backed up.
- ➢ I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- ➢ I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- ➢ I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- ➢ I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- ➢ Where personal data is transferred outside the secure school network, it must be encrypted.
- ➢ I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- ➢ I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- ➢ I will ensure that I have permission to use the original work of others in my own work
- ➢ Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- ➢ I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- ➢ I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Parent / Carer Acceptable Use Policy Agreement Template

New 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 digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

> ➢ that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
> ➢ that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
> ➢ that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Student(s) Name(s)	

As the parent/carer of the above student(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son(s) has/have signed an Acceptable Use Agreement and received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my son to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed [   ]   Date [   ]

Approvals
 	
▪ Signatures:
  Principal
 	
                    Chair of Governors
 	
▪ Date of approval by Governors:
 	
▪ Date of next annual review:
	
	_____
	
	_____
	
	____ / ____ / _____
	
	____ / ____ / _____