Introduction
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

In order to keep young people safe it is fundamental that the use of ICT both in and outside of the school community is used correctly in order to protect young people from harm. Therefore this policy applies to the Head Teacher and to all members of staff employed by Mary Immaculate High School. This policy is designed to not only safeguard pupils from harm but also protect staff in terms of both e-safety and their use of ICT both in and outside of the classroom.

Roles and Responsibilities
Mary Immaculate High School strongly recognises the educational value of the use of ICT both in and outside of the classroom in order to support teaching and learning. However Mary Immaculate High School realises there is great temptation which comes with this technology in the form of misuse. Therefore everyone within the school community has a direct role and responsibility to play in ensuring suitable e-safety provision is provided for all students in our care. These roles and responsibilities are outlined below:

Board of Governors
The head teacher and at least another member of the board should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff so that immediate action may be taken. It is also the direct responsibility of the board of governors to ensure that there is a system in place in order to allow for the monitoring and support of those in the school community who carry out the internal e-safety monitoring role. The board of governors is also responsible for ensuring the school's approach to sexting is reflected in its child protection policy.

Head Teacher
The Head Teacher has a duty of care for ensuring the safety of pupils within the Mary Immaculate High School. However the day to day responsibility for e-safety is ultimately delegated to the school's E-Safety Officer. The Head Teacher however does have a direct responsibility for making sure the school's stakeholders are fully aware of the e-safety provision which is provided by the school.

Child Protection Officer
It is important to remember technology provides additional opportunity for child protection issues to occur and therefore the Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from the following situations:

- Sharing of personal data
- Access to illegal / inappropriate material
- Inappropriate on-line contact with strangers
- Potential or actual incidents of online grooming
- Cyber-bullying

In the event of the E-Safety Officer being absent all e-safety matters automatically pass over to the Child Protection Officer who is expected to deputise in their place for the duration of their absence.

Middle Leaders
Middle Leaders are responsible for ensuring:

- Policies and procedures are in place in order to deal with any e-safety incidents which may occur
- Make sure departments / faculties are aware of the procedures which should be followed in the event of an e-safety incident occurring
- Participate in any e-safety training events which may take place. This training may be provided through events put on by:
    - Local Authority
    - E-Safety Organisations

- School E-Safety Officer

From time to time Middle Leaders may be expected to use the knowledge acquired at these events in order to help lead whole school e-safety training event for both staff and students.

E-Safety Officer

The E-Safety Officer takes the day to day responsibilities for e-safety away from the Head Teacher and has a direct role in establishing and reviewing the school's e-safety policies. The E-Safety Officer will be a member of the technical support team and within this role they're expected to:

- Take the lead in monitoring and identifying any e-safety incidents which occur and liaise with the Senior Leadership Team / DSP and any relevant bodies in the school community in order to deal with these incidents quickly and effectively
- Provide the middle leadership team with regular monitoring reports in regards to e-safety provision
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and ensure DSP is informed
- Provide training and advice for staff in regards to key e-safety matters
- Meet regularly with the Network Manager, Assistant Head Teachers with responsibility for KS3 and KS4 and DSP in order to discuss current e-safety issues, review incident logs, filtering logs and change access controls if necessary
- Produce, review and monitor the school's e-safety literature
- Liaise with Assistant Heads of Year to map and review the school's e-safety curriculum within the PHSE framework
- Work towards achieving and maintaining the 360 e-safety charter mark

Network Manager

The Network Manager is expected to support the e-safety officer in their role and help them deal with any e-safety incidents which occur. In order to this the Network Manager is expected to:

- Ensure the technical infrastructure of the school's IT systems are secure and not open to misuse or malicious attack
- Mary Immaculate High School meets the e-safety technical requirements set out by National Government
- Make sure that access to the network and to school devices only takes place through a properly enforced password protection system
- A filtering policy is in place and is applied and updated on a regular basis
- They keep up to date with e-safety technical information in order to effectively carry out their role and to inform and update other users as required
- That the use of the Network, Email, Internet and VLE are all regularly monitored in order to ensure that any misuse can be reported as necessary
- They implement and maintain the School Technical Security Policy
- Review regularly the school ICT and security systems
- Discuss security strategies with the Local authority
- The contact details on the school website contain the school address, e-mail and telephone number and staff / student personal information is never published
- Provide parent / carers with regular updates in regards to e-safety matters
- Ensure e-safety rules are posted and maintained in all networked computer rooms
- Ensure m-learning devices are secure and that pupils can only access appropriate materials

Teaching and Support Staff

All teaching and support staff at Mary Immaculate High School have a direct responsibility for ensuring the e-safety provision of students in their care. Therefore within this responsibility teaching and support staff are responsible for ensuring:

- They have an up to date awareness of e-safety matters
- They are aware of the school's current e-safety policy and ICT practices

- They have read and understood the **Staff Acceptable ICT Use Policy Agreement (Appendix A - Acceptable ICT Use Agreements)**
- They directly report any misuse or problems in regards to e-safety to the E-Safety Officer
- That any digital communications which take place with pupils, parents and carers are on a strictly professional level and only carried out by using official school systems / accounts
- E-safety issues are embedded in all aspects of the curriculum and other activities where appropriate
- They show full compliance to the school's Data Protection and Data Transfer policies
- Pupils understand and follow the school's e-safety and acceptable ICT use policies
- Pupils have a good understanding of the research skills which are needed in order to avoid plagiarism and copyright abuse
- They monitor the use of digital technologies in their lessons and fully adhere to school policy
- Personal social media accounts are fully protected and the content on them does not bring Mary Immaculate High School into disrepute
- They are not "friends" with any pupils on social media sites and it is also strongly advised that is the same case with parents and carers
- Where contact with students is required through the use of a phone such as with a school trip, a school mobile phone is used at all times

Pupils

Before any pupil starts at Mary Immaculate High School they are expected to sign our **Pupil ICT Acceptable Use Policy (Appendix A - Acceptable ICT Use Agreements)**. In addition to pupils signing this agreement we expect them as learners to:

- Have a good understanding of the importance of fully adhering to copyright law
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know and understand the policies in place on the use of mobile devices and digital photography
- Realise and understand the importance of adopting good e-safety practices both in and outside of the school community
- Ensure that any mention of Mary Immaculate High School on social media sites doesn't bring the school into disrepute
- Be aware that any misuse of technology connected to e-safety can lead to their place in the school being terminated and the police can also be involved if necessary
- Immediately tell a teacher if they receive an offensive e-mail
- Not to reveal personal details of themselves or others in school-related e-mail communications, or arrange to meet anyone without specific permission;
- Ensure that any emails sent to external organisation are written carefully and authorised before they are sent

Parent and Carers

As a school we understand and recognise that parents / carers may only have a limited understanding of the e-safety risks and issues which are associated with the use of technology both in and outside of the classroom. Therefore the school seeks to provide e-safety information to parents and carers through the following mediums:

- Curriculum activities
- Letters
- Parent evenings
- School app
- Social media posts
- E-safety seminars
- School website

In addition to pupils having to sign the **Pupil Acceptable ICT Use Policy (Appendix A - Acceptable ICT Use Agreements)** parents and carers are also required to sign this agreement and are responsible for ensuring their child fully adheres to the content which is outlined within this policy.

Curriculum
Where technology is used within the curriculum e-safety should be an automatic focus in all lessons in order to ensure it is used correctly so that both staff and pupils are protected through its use. The e-safety curriculum which Mary Immaculate High School provides is as follows:

- E-safety is a fundamental aspect of the school's PSHE program and DCF framework
- Key e-safety messages are reinforced once a term as part of the school's assembly program
- Pupils should be taught in all lessons to be critically aware of any information they may find online
- Staff should act as good role models in their use of digital technologies
- Processes are in place in order to deal with any inappropriate content which pupils may gain access to
- In lessons where the use of technology is pre-planned it is best practice that pupils are guided in terms of how to use the piece of technology safely and in a mature adult manner
- A dedicated section for e-safety issues is available on both the school website and school app

It is accepted that from time to time pupils may need to research certain topics for a particular subject which might be blocked for reasons such as drugs, racism etc. In such situations staff can request that the Network Manager unblocks a website(s) for a specified period of time. Any requests which staff make should be documented by the **Technical Support team (Appendix B – Online Forms).**

CPD
It is fundamental that all staff receive regular and relevant e-safety training so that they are fully protected and understand their responsibilities in regards to e-safety matters. Therefore at Mary Immaculate High School we provide staff with the following CPD for e-safety matters:

- Induction training ensures staff are fully aware of the school's e-safety program and acceptable ICT use policies
- Regular audits are carried out in order to assess the training needs of staff
- Any amendments to this policy will be presented to staff and discussed further on INSET days if necessary
- The E-Safety Officer will liaise with the Senior Leadership Team to provide guidance, advice and training to individuals are requested
- Opportunity for the E-Safety Officer to attend external e-safety events
- E-safety will appear in the INSET programme annually
- Open invitation for staff to attend any e-safety seminars which are put on by the E-Safety Officer and by members of the Senior Management Team.

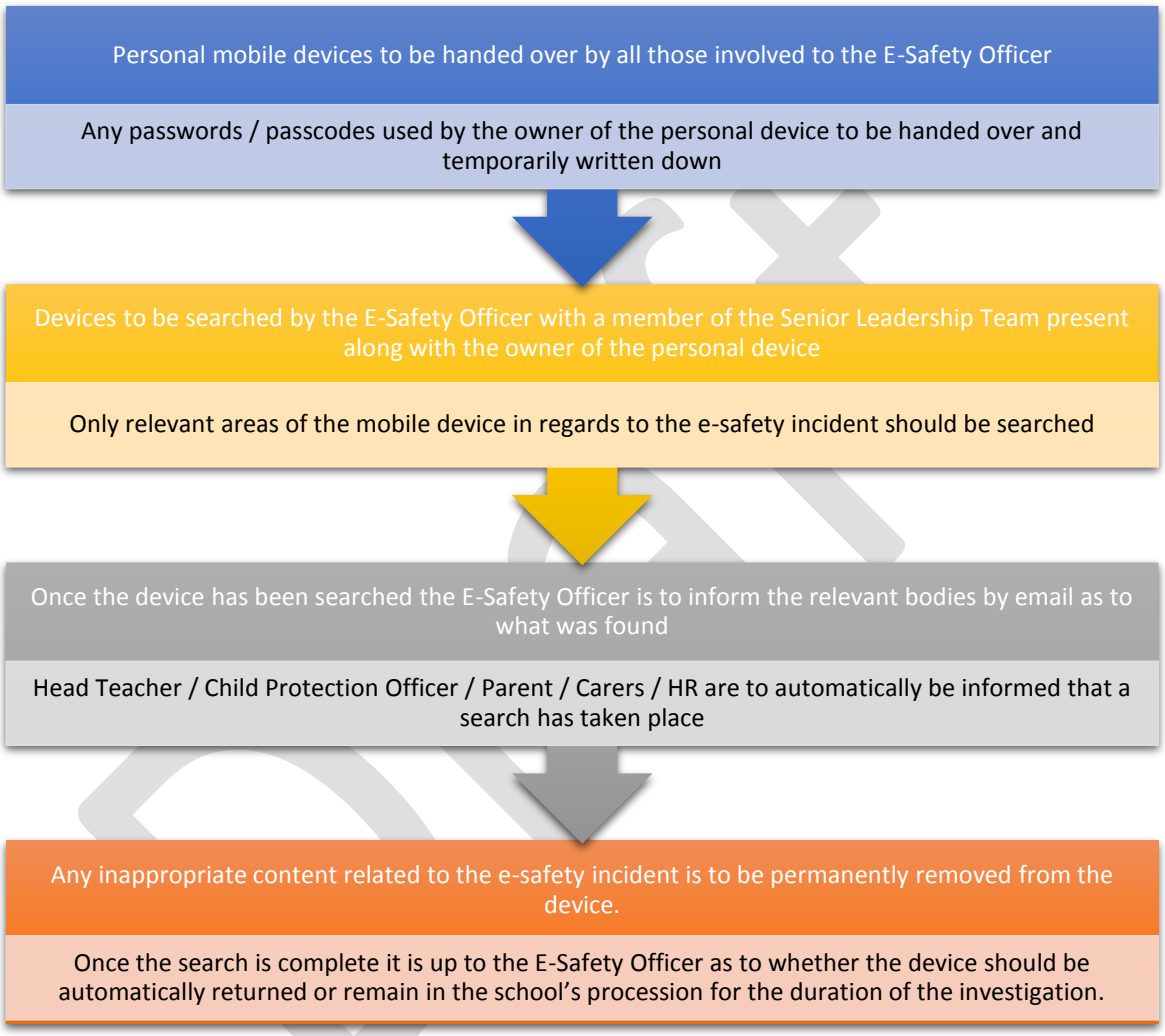
Use of Digital Videos and Images
Digital imaging technology can add real value to both teaching and learning within the school environment. However staff, parents / carers and pupils all need to be aware of the harm these technologies can cause with or without intent to cause harm. Therefore the following policies are in place in order to protect all members of the school community:

- When using digital cameras, camcorders and iPads staff should make sure pupils are aware of the risks which are connected to their use
- Parents / carers are welcome to take photos of their children at school events but should not publish these images on social media sites
- Staff should only take photos and videos of students for a specific purpose with the use of school technology. Personal devices should not be used
- Care should be taken when taking photos or making videos that pupils are dressed appropriately and are not participating in activities which can bring the school into disrepute
- Pupils must not use, publish or share images / videos of other pupils without their permission

- Permission will be obtained from parents / carers in order to publish images and videos of pupils through official school communication channels

Searching of Devices

The Education Act of 2011 increased powers further for Head Teachers with regards to the searching for and of electronic devices and the deletion of data. Therefore in the event of an e-safety incident taking place which involves mobile devices the following procedure needs to be followed when searching the devices of pupils:



Following an examination of an electronic device, if the e-safety officer has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the e-safety officer must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. If inappropriate material is found on the device it is up to the e-safety officer to decide whether they should delete that material or retain the device as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

Staff who are accused of inappropriate use of their own personal device will be given the opportunity to follow this procedure or the matter will be directly referred to the Police.

Social Media

Mary Immaculate High School recognises the importance of interacting with the school community through social media channels. However in order to fully protect the staff who maintain and use these channels the following policies are in place:

- The only social media channels which are to be used by staff in order to represent Mary Immaculate High School are as follows: Facebook & Twitter.
- All social media channels must be registered through the following email address: facebook@maryimmaculate.cardiff.sch.uk
- The email address facebook@maryimmaculate.cardiff.sch.uk is managed and moderated by the Network Manager
- Any communications which are deemed not acceptable on these social media channels will be passed over by the Network Manager to the Head Teacher who will decide what action to take
- Any members of staff who wish to use these social media channels and represent Mary Immaculate High School will need to adhere to the **School's Acceptable Social Media Use Policy Agreement (Appendix A -** Acceptable ICT Use Agreements**)**
- Students' full names will not be used unless prior parental consent has been agreed, for example, in the case of rewards

Managing Emerging Technologies

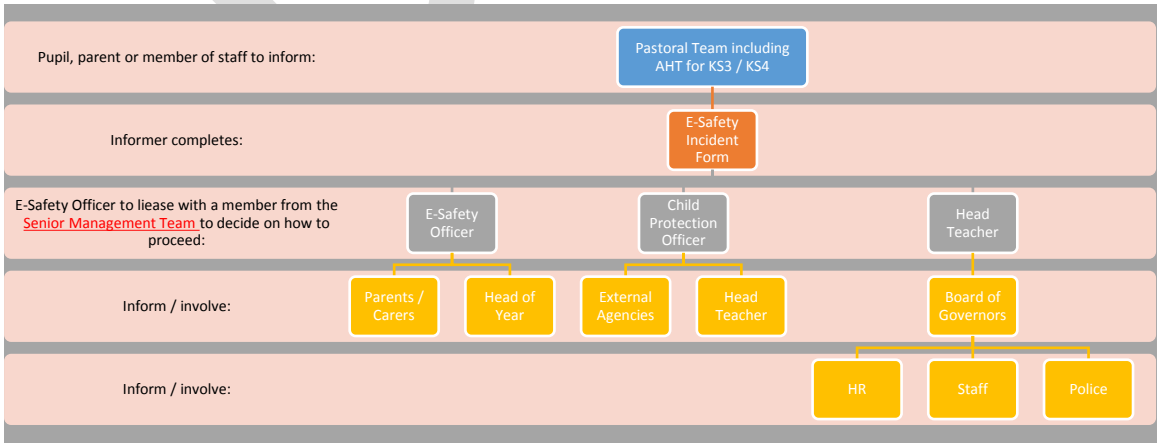
Mary Immaculate High School is fully aware of the benefits technology can bring to the school environment. Therefore emerging technologies will be examined by the E-Safety Officer / Network Manager and by relevant staff in order to assess the educational benefits and risks the technology may bring. The E-Safety Officer / Network Manager / Head of DCF is responsible for deciding whether the emerging technology is suitable for school use, a risk assessment will be completed.

Actions and Sanctions

In the event of an e-safety incident occurring for either a pupil(s) or member of staff(s) **Appendix C - Possible Actions and Sanctions** outlines the possible actions and sanctions which may be taken. These actions and sanctions are deemed as possible actions and sanctions as each e-safety incident is different from the other which means discretion might need to be applied in certain situations. Any final decisions in regards to what actions and sanctions should be applied in the event of an e-safety incident occurring rest with the E-Safety Officer, the Head Teacher and the Board of Governors.

Pupil E-Safety Incident

It is your responsibility as a member of staff to follow the following process in the event of a pupil e-safety incident taking place:



Within the diagram shown above it is very clear that once you have reported an e-safety incident to the E-Safety Officer you must immediately complete an E-Safety Incident Form **(Appendix B – Online Forms)** in order to protect yourself and the E-Safety Officer. The E-Safety officer will be responsible for emailing you a copy of

the form you need to complete. Based on the information you give to the E-Safety Officer they will decide how to further precede with the incident which has occurred.

Member of Staff E-Safety Incident
As a member of staff if you feel you are being bullied online you should immediately seek support and guidance from the Senior Management Team as to how to deal with such an incident. In order to ensure you are fully protected in such an incident occurring you should undertake the following actions:

1. Don't respond or retaliate to any cyberbullying incidents, no matter what the circumstances are
2. Report any incidents which occur with the Senior Management Team and act on the advice they give you
3. Gather evidence of the abuse; take screenshots of messages or web pages and record the time and date as to when they happened

Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures. However if the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the Police as online harassment is a crime which can't be tolerated.

The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. This organisation is recommended by South West Grid for Learning. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues. The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more. If you need to contact this helpline the number you need to ring for the Teacher Support Network in Wales is 0800 085 5088.

Policy Approved: [Enter here]
Policy Review Date: December 2017
Next Review December 2018

Appendices

Appendix A – Acceptable ICT Use Agreements
Appendix B – Online Forms
Appendix C – Possible Actions and Sanctions

Appendix A
Acceptable ICT Use Agreements

Pupil Acceptable ICT Use Policy Agreement

Mary Immaculate High School strongly believes in the educational value of the use of ICT in the classroom and recognises its potential in supporting both teaching and learning. However any inappropriate misuse of ICT both in and outside of the school community is strictly prohibited. Therefore in order to qualify for access to ICT services in the school pupils must read and follow the following agreement:

1. Personal Responsibility
As a representative of the school you accept personal responsibility for reporting any misuse of the network to a member of staff.

2. Acceptable Use
The use of ICT services must be in support of education and research in accordance with the educational objectives set out by Mary Immaculate High School.

3. Privilege
The use of ICT is a privilege and any inappropriate misuse can result in that privilege being withdrawn either permanently or for a period of time.

4. Security
If you identify a security problem with any piece of technology in the school, you must notify your ICT / Computer Science teacher straightaway and shouldn't demonstrate the problem to any other pupils.

5. Vandalism
Any malicious attempt to harm or destroy any equipment or data will result in disciplinary action being take and any deliberate damage to equipment must be paid for by yourself.

6. Electronic Mail
Email facilities are provided by the school through the Microsoft Office 365 suite. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden.

7. Chat Services
Pupils are not permitted to use any chat facilities which are available on the Internet.

8. Internet Search Engines
Pupils are required to use Internet search engines responsibly. If pupils are found to be searching for material which is unsuitable and is in breach of this policy they will face disciplinary action.

9. Executable, Music and Video Files
Pupils are strictly forbidden from introducing executable files (e.g. '.exe, .cmd, .bat, .bin') to the network as these in some cases can contain harmful viruses.

10. Social Networking Sites
Pupils are not permitted to use social networking sites in school hours unless it is for academic purposes such as research.

Staff Acceptable ICT Use Policy Agreement

Mary Immaculate High School strongly believes in the educational value of the use of ICT in the classroom and recognises its potential in supporting both teaching and learning. Any inappropriate misuse of ICT both inside and outside of the school community which brings the school reputation into disrepute is strictly prohibited and may result in disciplinary action being taken.

1. Personal Responsibility
As a representative of Mary Immaculate High School you accept personal responsibility for reporting any misuse of the network to the Network Manager. You are also responsible for ensuring any communications which take place between yourself, pupils and parents / carers is of a strictly professional nature. These communications should only take place on official school systems.

2. Acceptable Use
The use of ICT services in any lesson must be in support of education and research in accordance with the educational objectives set out by Mary Immaculate High School. Where technology is used in a lesson you must fully comply with the school's ICT and E-Safety Policy. **Staff must not remove pupil, parental or staff data from school premises. Where devices are used (e.g. laptops) they must always be encrypted.**

3. Privilege
The use of ICT is a privilege for pupils and any inappropriate misuse can result in disciplinary action being taken. When technology is used in a lesson you are responsible for ensuring pupils fully understand the consequences of any misuse.

4. Security
If you identify a security problem with any piece of technology in the school, you must notify the Network Manager at the earlier opportunity.

5. Electronic Mail
Email facilities are provided by the school through the Microsoft Office 365 suite. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. You must immediately inform your Line Manager at the earliest opportunity of any form of communication through email which makes you feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature. You must not respond to any such communications.

6. Chat Services
Whilst you are on the school site using school technology you are not permitted to use any chat facilities which are available on the Internet.

7. Internet Search Engines
You are required to use Internet search engines responsibly and appropriately.

8. Executable, Music and Video Files
Members of staff are strictly forbidden from introducing executable files (e.g. '.exe, .cmd, .bat, .bin') to the network without the permission of the Network Manager as in some incidents these files can contain harmful viruses.

9. Social Networking Sites
You are not permitted to use social networking sites in school hours unless it is for academic purposes or to represent Mary Immaculate High School. If you wish to represent Mary Immaculate High School on Social Media Sites you will need to fully comply with the school's Acceptable Social Media Use Policy Agreement.

Social Media Acceptable Use Policy Agreement

Mary Immaculate High School recognises the importance of interacting with the school community through social media channels. However in order to fully protect the organisation and the staff who maintain and use these channels the following agreement must be read and followed:

1. Personal Responsibility
As a representative of Mary Immaculate High School you accept personal responsibility for anything you post on any social media sites which represent the school.

2. Acceptable Use
Facebook and Twitter are the only social media sites which are to be used in order to represent Mary Immaculate High School.

3. Privilege
The use of representing Mary Immaculate High School through social media sites is a privilege and any inappropriate misuse can result in disciplinary action being taken. The only email address which is to be used with any social media account for Mary Immaculate High School is facebook@maryimmaculate.cardiff.sch.uk

4. Security
Each of the authorised social media accounts have been set up and are ran by the Network Manager. Therefore you are not authorised to change any of the settings they have put in place. Any settings put in place by the Network Manager are designed to protect you and Mary Immaculate High School.

5. Personal Information
When posting any type of communication through social media site you must ensure that all times no personal information is made public. Any posts which have to contain an email address should contain a school email address.

6. Personal Opinions
Any posts through social media sites should be to do with generic information in regards to the school and should not contain any personal opinions or views which could bring Mary Immaculate High School into disrepute.

7. Media
Any media through the use of images or videos which are uploaded to these social media sites should be of a strictly professional nature and should fully adhere to the guidelines set out in the school's ICT and E-Safety Policy document.

8. Direct Communication
If parents / carers choose to interact with these social media channels and require a direct response to a query they should be directed to an official school email address if a longer response is required. Any interactions with parents / carers should be of a strictly professional nature. Interaction with pupils is strictly prohibited.

9. Endorsement
On many of these social media channels if can be tempting to "follow", "retweet" or "like" a particular post, however great care should be taken when doing this as one of these actions could be seen as an actual official endorsement which could bring the school into disrepute. Therefore these actions should be left to the Network Manager in order for them to implement.

10. Unsuitable Communications
If you are using one of these social media sites and representing Mary Immaculate High School it is your responsibility to immediately notify the Technical Support Team if you feel a communication which has been received is unsuitable.

Appendix B
Online Forms

E-Safety Incident

If an e-safety incident is notified to yourself by a pupil or by another member of staff you are automatically required to report it to the school E-Safety Officer. Once you have reported the incident to the school E-Safety Officer you are required to complete a form which will be emailed to you by the e-safety officer. The emailed form will contain the following questions:

- When were you first notified about this incident?
- When did you notify this incident to the e-safety officer?
- Who does this incident involve?
- What information did the e-safety officer give you?
- What actions were decided with the e-safety officer?
- What is your name and job title?

This information will be captured electronically along with a time and date stamp being taken.

Block a Website

If you come across an inappropriate website during a lesson which you are delivering you are required to complete an online form which will contain the following questions:

- What is the address of the website you want blocked?
- Why should this website be blocked?
- How long do you want this website to be blocked for?
- What is your name and job title?

On submission of the above information the Network Manager will process your request in a reasonable amount of time and their decision is final as to whether the website you have requested to be blocked can be authorised or not.

Unblock a Website

If you wish for a specific website to be unblocked from the school's filtering system you must complete an online form which will contain the following questions:

- What is the address of the website you would like unblocked?
- Why do you need this website to be unblocked?
- How long do you want this website to be unblocked for?
- What is your name and job title?

On submission of the above information the Network Manager will process your request in a reasonable amount of time and their decision is final as to whether the website you have requested to be unblocked can be authorised or not.

Appendix C
Possible Actions and Sanctions

In order to protect both staff and pupils from harm in terms of e-safety this appendix outlines what actions are allowed and prohibited within Mary Immaculate High School. It is worth noting that this section is entitled "possible actions and sanctions" as each e-safety incident is different and as such these tables should merely be used / act as a guide for consistency purposes.

Actions - Pupils

	Allowed	Allow at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X			
Use of mobile phones in lessons			X	
Use of mobile phones in social time	X			
Taking photos on personal devices			X	
Use of personal mobile devices			X	
Use of messaging apps				X
Use of social media		X	X	
Use of blogs			X	

Actions - Staff

	Allowed	Allow at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	X			
Use of mobile phones in lessons		X		
Use of mobile phones in social time	X			
Taking photos on personal devices		X		
Use of personal mobile devices	X			
Use of messaging apps		X		
Use of social media		X		
Use of blogs		X		

Sanctions – Pupils

Incident	Discipline Stage				Inform Parent / Carers	Inform Network Manager	Inform Police (As required)
	1	2	3	4			
Unauthorised use of non-educational sites during lessons e.g. Games	X						
Unauthorised use of mobile device	X						
Unauthorised use of social media	X						
Unauthorised use of downloading or uploading files			X		X	X	
Attempting to access the school network by using another pupil's account without permission			X		X	X	
Attempting to access the school network by using the account of a member of staff				X	X	X	
Corrupting or destroying the data of other users				X	X	X	
Sending a digital communication which is regarded as offensive, harassment or of a bullying nature				X	X	X	X
Continued infringement of sending inappropriate digital communications				X	X	X	X
Actions which could bring the school into disrepute				X	X	X	
Using proxy sites or other means in order to bypass the school's filtering system				X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X	
Deliberately accessing or trying to access offensive or pornographic material				X	X	X	X
Receipt or transmission of material which breaches copyright law			X		X	X	

1= Discussion with classroom teacher / form teacher.
2= Head of Department / Head of Year Referral.
3= Head of Year / Head of Key Stage Referral / Report to E-Safety Officer.
4= Inform Learning Walking / Report to E-Safety Officer.

Sanctions - Staff

Incident	Refer to Line Manager	Refer to Network Manager	Refer to Head Teacher	Refer to Board of Governors & HR	Refer to Police
Inappropriate use of the Internet	X	X			
Unauthorised use of downloading / uploading files	X	X			
Using another person's account without permission in order to access the network		X	X		
Careless use of personal data	X	X			
Deliberate actions to breach data protection		X	X		
Deliberate corruption of files and assets			X	X	
Sending electronic communications which are deemed offensive, harassment or of a bullying nature			X	X	
Using personal online communication channels in order to interact with current students			X		
Actions which could compromise a staff member's professional standing			X		
Actions which could bring the school into disrepute			X		
Using proxy sites or other means in order to bypass the school's filtering system	X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		
Deliberately accessing or trying to access offensive or pornographic material				X	X
Receipt or transmission of material which breaches copyright law			X	X	