BELFAST MODEL SCHOOL FOR GIRLS
Achievement for All

Pupil eSafety Policy

Agreed by Board of Governors: *October 2016* **To be reviewed:** *Annually by Digital Leaders*

Rationale

*Belfast Model School for Girls provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce risks. This **Pupil eSafety policy** explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the Internet and digital technologies for educational, personal and recreational use*

The Internet and other digital technologies are powerful tools, which open up new opportunities for everyone. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. 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. These technologies can **stimulate discussion**, **promote creativity** and **increase awareness** of context **to promote effective learning.**

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to, loss of, sharing of personal information;
- The risk of being groomed online;
- The sharing or distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyberbullying;
- Access to unsuitable video or games;
- Exposure to inaccurate, unreliable or poor quality information;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive "online time" which may impact on the social and emotional development and learning of young people.

Many of these risks reflect situations in the real world and it is essential that this eSafety policy is read, understood and relates to other school policies; **Anti-Bullying**, **Behaviour** and **Child Protection**. As with all risks, it is impossible to eliminate these risks completely. It is therefore essential that we build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with them should they occur.
This policy applies to **all pupils of the Belfast Model School for Girls** who have access to the school ICT networks, hardware and software, both in and out of school. Any user of the school ICT networks must adhere to and sign a hard

copy of the **Pupil Acceptable Use Policy** available at the end of this document. This policy applies to all use of the Internet and devices that have Internet access or digital communication methods, such as email, text messaging, group chat and social media.

Note: The Belfast Model School for Girls' operates two distinct networks within the school.

- *The C2K network (supported by DENI) is managed by Capita, who are responsible for the filtering of the network. This is managed within the school by the C2k Manager **Mr N Adams**.*
- *A Legacy network, with a C2K internet connection, managed by the school's Network Manager **Mr F Clarke** and overseen by Principal **Mr E Wright***

Stakeholder's roles & responsibilities

Children and young people should have an entitlement to safe Internet access at all times. A pupil eSafety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education (Principal, Board of Governors, eSafety Lead Teacher, Teachers, Support Staff, Parents, and the Pupils themselves).

This section outlines the roles and responsibilities for eSafety of individuals and groups within the Belfast Model School for Girls.

Board of Governors are responsible for the approval of the eSafety policy and for reviewing the effectiveness of the policy. A member of the Board of Governors has taken on the role of **Safeguarding**. This role includes

- Meetings with the ICT Manager and and eSafety Lead Teacher.
- Regular monitoring of eSafety incident logs.
- Reporting to relevant Governors in committee meetings.

Mr E Wright (Principal) is responsible for ensuring:

- The safety (including eSafety) of all members of the school community.
- Effective monitoring systems for eSafety are set up.
- Establishing and reviewing the school's eSafety policies and documents (with the eSafety Lead Teacher)
- Ensuring that the relevant staff members are trained in Child Protection and the issues that may arise from incidents involving eSafety.

Mrs C Barkley-Smith (eSafety Lead Teacher) takes day to day responsibility for eSafety issues and has a leading role in:

- Linking in with the Principal and all staff on issues related to eSafety.
- Providing training and support for staff on eSafety.
- Keeping an eSafety log of incidents.
- Coordinating and reviewing the eSafety education programmes in school.
- Running the Year 10 Digital Leaders programme.

Mr Felim Clarke (ICT Manager) is responsible for ICT Infrastructure and his role includes

- Ensuring the network is secure and meets eSafety technical requirements.
- The school's filtering policy is applied and updated on a regular basis.
- Keeping up to date with eSafety technical information.
- Monitoring the use of the school equipment for misconduct or misuse, including the use of email, in order that incidents can be reported to the eSafety Lead Teacher and the Principal for investigation or action.

Teaching & Support Staff are responsible for ensuring that:

- eSafety is embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's eSafety and acceptable use policies, and ensure pupils know the channels to follow if they are unhappy about an incident relating to eSafety.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- ICT activity in lessons, extracurricular and extended school activities is monitored and safe.
- Where Internet use is pre-planned, pupils are guided to suitable sites, and that there processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Deliver eSafety training as directed by a whole school activity, including Form Period and Learning for Life and Work.

Parents/Carers play a crucial role in ensuring that their children understand the need to use Internet enabled and mobile devices in an appropriate way. The school will therefore take opportunities to help your parents understand these issues. Parents and Carers will be responsible for:

- Reading this policy along with the student, and agreeing to the school's eSafety policy.
- Co-signing the Pupil Acceptable Usage Policy.
- Seeking support and guidance from the school on eSafety advice and training by accessing the school's website and reading its social media messages.

Dealing with Issues

*This policy links with our **Anti-Bullying Behaviour Policy**. Belfast Model School for Girls aims to provide positive praise, encouragement and rewards for the things you do well and work hard for. If a school rule is broken, each case will be dealt with individually and the sanction based on the facts of the event. The Principal works along with the Board of Governors to decide on a course of action: Sanctions can be up to and including suspension or expulsion from school, depending on the circumstances.*

Your responsibility as a pupil of Belfast Model School for Girls

- You are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which you will be required to sign before being given access to school systems. Your Parents/Carers will be required to read through and co-sign this with you.
- You must report abuse, misuse or access to inappropriate materials, and know who to report this to.
- It is important that you adopt responsible eSafety practices when using digital technologies both inside and out of school. This eSafety policy also covers your actions outside of school if the activity is related to the Belfast Model School for Girls
- You must not partake in any activity online that is bad for your own reputation, the reputation of your family or your school.
- You must not participate in any form of Cyber Harassment or Cyberbullying.

The role of eSafety in Education

As a pupil of Belfast Model School for Girls, you

- receive a planned eSafety and Digital Citizenship programme as part of PSHE, and in ICT across all year groups. It is regularly revisited and adjusted with trends and developments in technology to ensure it is up to date.
- are protected by a rigorous filtering policy to ensure that your access to online material is both safe and age appropriate. Pupils are also aware that all internet use at school is tracked and logged.
- understand the need for the Pupil Acceptable Use Policy and are encouraged to adopt safe and responsible attitude towards the use of technology both inside and outside of school.
- are taught to be critically aware of the materials/content accessed online and guided to validate the accuracy of the information.
- are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- are taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

The role of eSafety in Digital Communication

Digital communication covers all forms of communication (such as emails, blogs, text messaging, instant messenger) through Mobile or Internet enabled devices. These devices included Smartphones, PC's, Laptops and Tablets.

As a pupil of Belfast Model School for Girls, you

- understand that any form of digital communications with other pupils and staff (for example: through a VLE forums or via email) are always of a professional manner and only carried out using official school systems.
- agree to your email being monitored by the ICT Manager.
- refrain for engaging in any form of unacceptable, abusive or inappropriate communication (through email, chat or text messaging) both inside and outside of school.
- should adhere to the rules and guidelines set out in the behaviour policy regarding mobile phone use in school.

The role of eSafety in Social Networking

Belfast Model School for Girls has an active website, Facebook and Twitter account which are used to inform, publicise school events and celebrate and share the achievement of pupils. This is an example of responsible use of social media when attached to the school community.

Pupils are not allowed access to social networking sites whilst in school, and Belfast Model School for Girls enforces this. At home, access to such sites are the responsibility of the parent. Parents are aware that some sites require a minimum sign up age of 13 Years.

As a pupil of Belfast Model School for Girls, you

- have a responsibility to yourself, your family and your school to act with the upmost respect and maturity when using social media.
- should not attempt to access any social networking sites on school equipment or on your own personal devices.
- should not attempt to add, accept or follow any member of teaching or support staff on any form of social media.
- will be aware that the school will investigate misuse of social networking if it impacts on the well-being of other pupils or staff.
- know that if inappropriate comments or items (including videos or images) are placed on social networking sites involving any member of the school community, then advice will sought from the relevant agencies, including the PSNI if necessary.

The role of eSafety for ICT Equipment

This section of the policy refers to acceptable use of the ICT equipment in Belfast Model School for Girls. All pupils must adhere to the following guidelines given below.

Removable Data Storage Devices

- Only school approved removable media should be used.
- All files downloaded from the internet, received via e-mail or provided on removable media (e.g. USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before being run, opened or copied/moved onto school network.

Cloud Storage

Pupil files and folders can be stored in the school's **GoogleDrive** in addition to the school's network. This means it can be securely accessed from any location removing the need to carry files on portable devices. It is also compatible with Mobile Devices, making work accessible to pupils without a computer at home.

Use of Own Equipment

Personal Devices

An overview of the devices permitted and for what activity is also included in the policy (See Appendix 2)

The school has introduced the use of Internet-enabled devices to support teaching and learning. These include PCs, laptops, iPads, tablets and personal mobile phones. Control of access to the Internet is managed by the school and must be enabled for each device. ***All 3G and 4G access must be disabled and will be checked by a member of staff to ensure all Internet access goes through the school C2K connection.***

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal files should not be stored on the local drives or the desktop of any school owned PCs
- All equipment should be treated with the upmost respect. Any accidents or breakages must be reported to a member of staff immediately

Passwords

- You must inform a member of staff immediately if you suspect your password has been traced, used or if it is forgotten.

C2K Specific

Internet Filtering

Belfast Model School for Girls has developed its own internet filtering policy, in addition to those filtered through the C2K connection. **Mr N Adams** and **Mr F Clarke** manage the filtering policy and can further amend the filtering based on the needs of the school. However there are a number of agreed locked down sites that can never be overridden by the school policy. *For example: Facebook, Instagram, Netflix and PirateBay*

Meru

Wireless Meru Wi-Fi provides increased wireless coverage and improved speed. Meru supports multiple devices and the school controls secure guest access, which allows the school to implement a 'bring your own device' policy.

Monitoring

All use of the school's Internet access is logged and the logs are regularly monitored by the school's external provider, as well as the ICT Manager. Whenever any inappropriate use is detected, it will be followed up by the eSafety Lead teacher and dealt with according to school policy. *(See also **Dealing with Incidents** section on page 4)*

Cyberbullying

Cyberbullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

Pupils may be subject to Cyberbullying via electronic methods of communication both in and out of school. Cyberbullying is also considered within the schools ***Anti -bullying policy****.*

Cyberbullying can take many different forms including:

- Sending threatening , abusive or inappropriate messages via email, text messages, Instant messaging (IM) , Group Chats, Direct Messaging (DM) Private Messages (PM) or chat rooms,
- Posting of nasty or upsetting comments about another user on social networking sites
- "Tagging" of users in defamatory or humiliating statuses, pictures or videos with the intention of causing embarrassment or distress.
- Online gaming – abuse or harassment of someone using online multiplayer gaming sites.
- Assuming another person's identity with the intention of causing trouble or mischief.

Whilst Cyberbullying may appear to provide anonymity for the bully, most messages can be traced back to their creator. Cyberbullying incidents can constitute a criminal offence.

If you feel you or someone else is the victim of Cyberbullying, you must speak to an adult as soon as possible, and follow the steps below

- Do not answer abusive messages but log and report them
- Do not delete anything, even if it is upsetting. The material is important evidence which may need to be used later.
- Do not give out personal details
- Never reply to abusive e-mails
- Never reply to someone you do not know
- Stay in public areas in chat rooms
- Delete and block accounts or users that you feel are of threat to you

Incident Reporting

Pupils in the Belfast Model School for Girls are encouraged to report incidents of Cyberbullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases. The school will also keep records of Cyberbullying incidents to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions. Pupils are reminded to refer to the "**Keeping Myself Safe Online"** and **"Smart Think"** posters that are displayed in classrooms around the school, and on the Interactive screens (See Appendix 3 and 4)

Appendix 1

BELFAST MODEL SCHOOL FOR GIRLS
Achievement for All

Pupil Acceptable Use Policy

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school ICT systems for personal or recreational use, for on-line gaming, gambling, Internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/iPod) in school at times that are permitted. This includes commuting to and from school, or to contact parents after participation in an extra- curricular activity. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving ICT equipment, however this may have happened.

Signed (Student / Pupil) …… **Date …….**

Signed (Parent / Guardian) …… **Date …….**

Appendix 2

Overview of Devices

Below is on overview of Personal Digital devices and their use in the school environment.

Communication Technologies		Permitted	Allowed with staff permission	Not Permitted
Mobile phones may be brought into school (but switched off)		**X**		
Mobile phones used in lessons for a planned activity			**X**	
Use of mobile phones in social time				**X**
Taking photographs on mobile devices				**X**
Use of PDAs and other educational mobile devices			**X**	
Use of school email for personal emails				**X**
Social use of chat rooms/facilities				**X**
Use of social network sites				**X**
Use of educational blogs			**X**	

Appendix Three

Appendix 4