METHODIST COLLEGE BELFAST
PREPARATORY DEPARTMENT

E-SAFETY POLICY

Introduction

The Preparatory Department recognises that ICT and the internet are powerful, worthwhile tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence.

Using ICT can benefit everyone in the school community, but it is important that students, staff and parents practise good eSafety.

eSafety is short for Electronic Safety and highlights the responsibility of school staff, governors and parents to mitigate risk through reasonable planning and action. eSafety covers all use of the internet and electronic communications through mobile phones, email, games consoles and wireless technology.

There is a 'duty of care' for any person working with children to educate them on the risks and responsibilities of using the internet and other technologies, and to ensure technical safeguards are maintained, while making technology accessible and of worthwhile educational value.

We know that some adults and young people will use these technologies to harm children. The SBNI Report *'An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland'* (January 2014) defines the risks around online safety under four categories:

- **Content risks**: exposure to harmful materials
- **Contact risks**: adult-initiated online activity including risk of grooming
- **Conduct risks**: bullying, entrapment or blackmail
- **Commercial risks**: exposure to inappropriate advertising, marketing schemes or hidden costs/fraud

Technical safeguards can partly protect users, but, no matter how rigorous such measures may be, they will never be completely effective. Therefore, education of all members of the school community in safe, effective practices is a key goal for the school.

Roles & Responsibility

eSafety is a whole-school issue and responsibility. Each school has a designated eSafety co-ordinator, who is part of a wider safeguarding team.

The e-safety co-ordinators are:

Downey House: Mrs D. Doherty
Fullerton House: Mrs C. Stewart

In Methodist College, Mr J. Lowry takes responsibility for Child Protection, including eSafety, on the Board of Governors.

The Designated Teacher in charge of Child Protection is Mrs A. Kennedy.

Communicating school policy

This policy is available from the school office for parents, staff and pupils to access when they wish.

All parents and pupils will receive a full copy of this policy on entry to the school, and a summary at the beginning of each subsequent school year.

All pupils and their parents will be required to sign that they have read, discussed and will abide by an Acceptable Use of the Internet agreement on an annual basis. They are reminded that all C2k systems are monitored and that security reports can be accessed by the Principal or designated senior member of staff.

Making use of ICT and the internet in school

The internet and other technologies are powerful resources that can enhance teaching and learning when used well. Technology is advancing rapidly and is now a huge part of everyday life, education and business.

We aim to use these resources effectively and appropriately in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into the next stage of their school career.

Some of the benefits of using ICT and the internet in schools may include
For students:

- Access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.

- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.

Professional development for teachers

Teachers are the first line of defence in eSafety and should ensure that pupils in their class are aware who they can approach with any concerns.

All teaching and non-teaching staff will receive regular training and support on recognising and reporting online safety issues within the school. Up to date eSafety training is currently delivered to all teachers and pupils on a two-year cycle.

The eSafety Co-ordinator and the Deputy Head in each school are responsible for ensuring that eSafety training is part of induction for new staff.

Each school's eSafety co-ordinator is responsible for the training of staff and can be approached for advice.

Education of pupils

Pupils should be taught to understand and use technologies in a positive way. They should be supported to develop safer online behaviours both in and out of school, to recognise unsafe situations and to respond to risks appropriately.

Online safety is actively promoted through the school through a progressive eSafety programme including workshops at each Key Stage and celebration of Internet Safety Day. A display giving advice on eSafety is displayed prominently.

It is also important that pupils learn how to evaluate internet content for accuracy and intent. This is built in to the delivery of the curriculum.

Students will be taught:

- the risks and benefits of the internet through an age-appropriate, relevant and engaging eSafety programme integrated across the curriculum.
- what to do if they are uncomfortable or unsure about something they have seen so that they feel confident online
- to use age-appropriate tools to search for information online.
- in key stage 2, to be critically aware of materials they read, and shown how to validate information before accepting it as accurate.
- in key stage 2, to acknowledge the source of information used and to respect copyright.

Education of parents

Information evenings for parents on online safety are delivered by an appropriate training provider on a two-yearly basis.

Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole; and takes the protection of school data and personal protection of our school community very seriously.

All computer access to the internet in school should be through the C2k network.

C2k provides an effective filtering system, as a result of which the following categories of websites should not be available in school:

- adult
- violence
- hate material
- illegal drug taking and the promotion of illegal drug use
- criminal skill/activity
- gambling

Resources or materials downloaded by teachers at home should come from sites that are accessible through the C2k network. Any downloaded material brought into school by pupils, parents or visitors should be checked first by the class teacher to ensure it is suitable for the classroom.

A case-by-case decision will be made by the Head of Department and the Principal on whether it is necessary to inform parents if a website is blocked or if an accessible resource is considered unsuitable for pupils.

If the school has retained otherwise unobjectionable printed materials downloaded from sites that are subsequently blocked by C2k or the College, a decision should be made on whether these resources should continue to be used. In making such a decision, the school should consider wider implications, such as whether continued use of such materials could be interpreted as endorsing an undesirable organisation or person. The approval of the Board of Governors may be sought if necessary.

If there is a potential breach of online safety, the URL should be reported to the eSafety Coordinator who will pass it on to the Head of the Preparatory Department and the College ICT Manager; the Head of the Preparatory Department or the Principal (or his deputy) should then report the matter immediately to the C2K Helpdesk. An up-to-date record of any potential breach will be recorded in an Online Safety Risk Register.

Any material found by members of the school community that is believed to be unlawful will be reported immediately by the Head of the Preparatory Department to the Principal, Board of Governors, parents and the Police. Where an incident is likely to involve media interest, the Department should be informed.

The security of the school information systems will be reviewed regularly by the ICT Manager in Methodist College and virus protection software will be updated regularly. Regular software and

broadband checks will take place to ensure that filtering services are working effectively. This protects the school network, as far as is practicably possible, against viruses, hackers and other external security threats.

Cloud storage means that secure access to C2k data and files is available at home for staff. This removes the need to carry such information on insecure data pens or portable devices.

Some safeguards that the school takes to secure our computer systems are:

- ensuring that unapproved software is not downloaded to any school computers.
- files held on the school network will be regularly checked for viruses.
- the use of user logins and passwords to access the school network will be enforced.

Mobile digital devices

Both Preparatory Departments have access to school-owned wireless technologies, e.g. iPads and other tablets, provide educational opportunities for both pupils and teachers.

However, management challenges are different from those afforded by desktop and laptop computers. At present we do not permit a 'Bring Your Own Device' system and only school owned tablets are permitted in for use by pupils.

All tablets should use the Meru Wireless coverage that allows controlled secure guest access.

Pupils are not permitted to download apps on to tablet computers, or to delete existing apps. Staff may download free apps that can be used to enhance teaching and learning experiences for themselves or their pupils. Any apps that need to be purchased should be requested from the College's ICT Manager in consultation with the UICT co-ordinator.

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyberbullying
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying behaviour and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. These are outlined in the school's mobile phone policy.

Pupils are not permitted to access the internet using a mobile phone in school.

The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

Staff should not use their personal mobile phones to take photographs or videos of pupils. They must use only cameras or devices provided by the school.

Email

All staff use the C2k email system internally to communicate. The C2k Education Network filtering system provides security and protection, ensuring that all messages are checked for viruses, malware, spam and inappropriate content.

Key Stage 2 pupils may use their school email account in supervised lessons to communicate with their teacher, each other or children in other schools as part of their work across the curriculum.

Staff and pupils should be aware that school email accounts should only be used for school-related matters. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

It is preferable that staff make contact with parents in person or by telephone through the school office. If a message is to be sent to a larger group, this should be done through the Schoolcomms system.

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate professionally. Personal email accounts should not be used to contact pupils or parents and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communication.
- Staff must tell a member of the senior management team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with it themselves.
- The forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the UICT curriculum and in any instance where email is being used within the curriculum or in class:

- in school, pupils should only use school-approved email accounts
- social emailing is unnecessary using their school account and is prohibited.
- pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with the problem themselves.
- pupils must be careful not to reveal any personal information over email; or arrange to meet up with anyone who they have met online.

The school website, published content and photographs

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published about the Preparatory Departments on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office

only.

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school.

However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material. The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons.

Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission.

All content on the school website is managed by the Methodist College web master, Ms Niamh Taylor or Mrs Nicola Pullin.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent.

On admission to the school parents/carers will be asked to sign a photography consent form. This consent form will outline the school's policy on the use of photographs of children, including:

- **How and when the photographs will be used.** Consent will cover the use of images in all school publications, on the school website, in newspapers as allowed by the school and in videos made by the school or in class for school projects.
- **School policy on the storage and deletion of photographs.** Electronic and paper images will be stored securely, and names of stored photographic files will not identify the child. Parents will be contacted annually to reconfirm consent while their child is at the school.

Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities) will focus more on the sport than the pupils.

For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group.

Staff are not permitted to take photos or videos of pupils on their own devices. If photos or videos are being taken as part of the school curriculum or in a professional capacity, school equipment must be used for this.

Events recorded by family members of the students such as school plays or sports days must be used for personal use only.

Pupils may take photographs of each other using only school cameras or tablets in a supervised lesson with their teacher's permission. Pupils are not permitted to use their own personal devices to take photographs or videos in school.

Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour. They will wear identification at all times and will not have unsupervised access to the pupils.

Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in. Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Any issues or sanctions will be dealt with in line with the school's child protection and positive behaviour policies.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes.

These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

Most social media sites have a recommended 13-years lower age limit which rules out their direct use by primary school age pupils. Pupils should not be allowed to access such sites in school on any device.

Social media sites have many benefits for staff, both for personal use and professional learning; however, staff should be aware of how they present themselves online. Staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory.

Official school blogs may be created as part of the school curriculum. They will be password-protected and run by a member of staff.

The school expects all staff and pupils to remember that they are representing the school at all times.

Cyber bullying

Cyber bullying, as with any other form of bullying behaviour, is taken very seriously by the school. The appearance of anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. However, most messages can be traced back to their creator and may constitute a criminal offence.

Cyber bullying can take many different forms and guises including:

- email
- instant messaging/chat rooms
- social networking sites
- online gaming

- mobile phone texts, videos and photo messages
- abusing personal information

If an allegation of cyber bullying is made, the school will:

- take it seriously.
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the 'bully.'
- record the incident on BCAF.
- provide support and reassurance to the pupil experiencing bullying behaviour.
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.
- If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will remove any harmful or inappropriate content that has been published, the service provider may be contacted to do this if they are unable to remove it. They may have their internet access suspended in school.

Managing emerging technologies

New technologies are emerging all the time. The school will risk-assess all new technologies before they are allowed in school; and will consider any educational benefits that they might have. The school aims to keep up-to-date with new technologies and to develop appropriate strategies for dealing with new technological developments.

Protecting personal data

Methodist College Preparatory Department believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital.

The school collects personal data from pupils, parents, and staff and processes it using ICT in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. Through effective data management we can monitor a range of school provisions and evaluate the well-being and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary. Pupil assessment, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs.

In line with the Data Protection Act 1998, the Freedom of Information Act 2000 and the General Data Protection Regulation 2018, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary

- process the data in accordance with the data subject's rights
- ensure that data is secure

There may be circumstances where the school is required, either by law or in the best interests of our students or staff, to pass information onto external authorities. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

This policy is guided by, and takes account of, DE circulars:

- 2007/1
- 2011/22
- 2013/25
- 2016/26
- 2016/27

This policy will be reviewed as appropriate