MOUNT LOURDES GRAMMAR SCHOOL

ICT Acceptable Use/Online Safety Policy

What is Online Safety?

The school has a duty to protect all its members and provide a safe, healthy environment. The term Online Safety is used to encompass the safe use of all online and digital technologies to reasonably protect all users from potential and known risk. Technology itself is only one aspect of this. Equally as important are the ways in which technology and the behaviours around it are managed. For safeguarding to be effective, Online Safety Procedures need to be clear, agreed and respected by everyone.

Online Safety also applies beyond the physical boundaries of the school and can impact on students and staff in this regard.

Why is Online Safety important?

Technology is constantly evolving with internet access becoming more mobile and accessible through a range of devices. Students are also using these technologies at an earlier age. It is our school's policy to address concerns and to safeguard against possible malicious use and overall Online Safety.

Online Safety and continuous professional development

The school will conduct regular Online Safety risk assessments with the aim of informing best practice in teaching, learning and continuous professional development. Online Safety risk assessment will also form the basis for auditing training needs of staff in relation to the safe and appropriate use of new technologies.

Staff will receive training in identifying Cyberbullying and in relation to their responsibilities in developing Online Safety.

Rules and Guidelines for Internet & Email use and safety

All internet & school email use is monitored by C2K.

School/C2k internet & email access is protected by a filtering policy which safeguards staff and students from viruses, spam and inappropriate content.

Under no circumstances are the following permitted:

- Misrepresenting the school in any way when using the facilities
- Gaining or seeking to gain unauthorised access to resources (hacking)
- Using the internet facility for illegal or fraudulent activities
- Sending or requesting messages or documents that are inconsistent with the school's policies and guidelines
- Using the facilities in ways that are considered to be malicious or unethical
- Accessing pornographic or otherwise unsuitable sites
- Disclosing passwords for school network and email accounts
- Revealing personal details such as address, telephone number or photograph to unknown individuals/forums.

Students are not permitted to access games on the Internet.

Students should only use the C2k email accounts within school.

Students should not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.

Students should never reveal their own or other people's personal details while online or arrange a face-to-face meeting with someone they only know through emails or the Internet.

Misuse of the Internet or email system will be dealt with in line with the school's Positive Behaviour Management and Procedures Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.

Rules and Guidelines for electronic communication devices including mobile phones

This policy sets out what is 'acceptable' and 'unacceptable' use of mobile phone and electronic communication devices by the whole school community.

It is recognised that it is the enhanced functions of many electronic communication devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation, and bullying.

Should electronic communication devices be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality.

- The recording, taking, and sharing of images, video and audio on any mobile phone or electronic communication device is prohibited.

- The school may retain any mobile phone or electronic communication device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, or bullying behaviour.
- Mobile phones and electronic communication devices will not be used in any way during lessons, assemblies or registration unless explicitly directed by a member of staff.
- Under no circumstances are Mobile phones and electronic communication devices permitted to be used in certain areas within the school site, e.g., changing rooms, toilets, and designated Health & Wellbeing areas.
- If a student breaches these rules, she will be asked to switch off her phone, and hand it into the Main Office, where her name will be recorded. The phone will be placed in a sealed envelope and must be collected at 3:25 p.m. Failure to comply with this guidance will be addressed in line with the school's Positive Behaviour Management and Procedures Policy.
- This policy also applies to students during school excursions, camps and extracurricular activities. Parents of students needing to use their mobile phones in exceptional circumstances, should negotiate arrangements with the relevant school staff, prior to departure from the school.
- In the event of images being taken on the school premises, without permission, they must be deleted in the presence of senior staff before the phone is taken off the school premises.
- If a student repeatedly breaches these rules, parents will be contacted and required to come into school to collect the device, or, the student may be asked to hand in their phone at the Main office each morning before 8.55a.m. It will be placed in a sealed envelope and returned to the student at 3.25p.m
- Mobile phones and electronic communication devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or electronic communication devices.
- Students have the opportunity to use personal electronic devices to support Learning and Teaching in the classroom as explicitly directed by and under the supervision of the class teacher or member of staff. Their use must comply with the school Bring Your Own Device Policy.

Rules and Guidelines for Electronic Device Safety at Home

- Only chat with people you know
- Never engage in chats that are offensive
- Do not video chat in bedrooms
- If someone becomes abusive, tell parents and report it

Cyberbullying

What is Cyberbullying?

- Cyberbullying is the use of ICT, commonly a mobile phone or the Internet, deliberately to upset someone else.
- It can be used to carry out all the different types of bullying behaviour, an extension of face-to-face bullying.
- It can also go further in that it can invade home/personal space and can involve a greater number of people.
- It can take place across age groups and school staff and other adults can be targeted.
- It can draw bystanders into being accessories.
- It includes threats and intimidation; harassment or 'Cyberstalking'; vilification/defamation; exclusion or peer rejection.
- Impersonation and unauthorised publication of private information or images and manipulation.
- Some Cyberbullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997.

Preventing/reporting Cyberbullying and promoting Online Safety

- Staff will receive training in identifying Cyberbullying and in relation to their responsibilities in developing Online Safety.
- Online Safety will be delivered through the PD Programme and also through KS3 ICT Classes.
- Students will be encouraged to report instances of Cyberbullying through the pastoral referral system.
- Students will be educated about Online Safety and Cyberbullying through a variety of means: assemblies, workshops, and lessons.
- Students & parents will sign the Acceptable Use/Online Safety policy before they are allowed to use school computer equipment and the Internet in school and parents will be asked to confirm that they have discussed its contents with their child.

- The school will use C2K filtering, firewall, anti-spyware software, anti-virus software and secure connections to safeguard the students.

- The school will provide information available via the school website on external reporting routes. For example, Childnet, ChildLine, CEOP, Safer Schools NI, ThinkUKnow and UK Safer Internet Centre.

Responding to Cyberbullying

Most cases of Cyberbullying will be dealt with through the school's existing Anti-Bullying Policy. However, some features of Cyberbullying differ from other forms of bullying behaviour and may prompt a particular response. The key differences are:

- Impact: the scale and scope of Cyberbullying can be greater than other forms of bullying

- Student displaying the bullying behaviour and student experiencing the bullying behaviour: the people involved may have a different profile to students who traditionally display bullying behaviour

- Location: the 24/7 and anywhere nature of Cyberbullying

- Anonymity: the person who is experiencing the bullying behaviour will not always know who is displaying the bullying behaviour

- Motivation: some students may not be aware that what they are doing is displaying bullying behaviour

- Evidence: unlike other forms of bullying behaviour, the student experiencing the bullying behaviour will have evidence of its occurrence

- It is possible that a member of staff may be experiencing the bullying behaviour and these responses apply to them too.

Support for the person experiencing the bullying behaviour

- Offer emotional support; reassure them that they have done the right thing in speaking out about their experience of bullying behaviour.

- Advise the person not to retaliate or reply. Advise the person to keep the evidence and take it to their parent or a member of staff.

- Advise the person to consider what information they have in the public domain.

- If hurtful or embarrassing content is being distributed, try to get it removed from the web. If the person who posted it is known, ensure they understand why it is wrong and ask them to remove it. Alternatively, contact the host provider and make a report to get the content taken down.

- In some cases, the person experiencing the bullying behaviour may be able to block the person displaying the bullying behaviour from their sites and services.

Investigation

- Members of staff should contact the Senior Teacher in charge of Pastoral Care, Mrs Jane McGeoghan in all cases of Cyberbullying.

- Staff and students should be advised to preserve evidence of any form of bullying behaviour. For example, save phone messages, record, or save/print online conversations, print or produce a screenshot of social network pages or print/save email messages.

- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact: the local police or CEOP (http://www.ceop.gov.uk/).

- Any allegations against staff should be handled as per the school's Safeguarding/Child Protection Policy.

- Contact the police in cases of actual/suspected illegal content.

Working with the student carrying out the bullying behaviour and applying sanctions

The aim of the sanctions will be:

- To help the person experiencing the bullying behaviour to feel safe again and be assured that the bullying behaviour will stop

- To hold the student displaying the bullying behaviour to account, getting them to recognise the harm caused and deter them from repeating the behaviour

- To demonstrate to the school community that Cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly

- In applying sanctions, consideration must be given to the type and impact of the bullying behaviour and the possibility that it was unintentional or was in retaliation

- The outcome must include helping the student displaying the bullying behaviour to recognise the consequence of their actions and providing support to enable the attitude and behaviour of the person displaying the bullying behaviour to change.

Evaluating the effectiveness of prevention measures

- A review of the Online Safety Policy and procedures will be undertaken in order to identify any areas for improvement. Staff, students and parents will be consulted as necessary.

- Staff training needs will be identified and actioned in the School Development Plan.

The use of social networking and online media

This school asks its whole community to promote the 3 common approaches to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos, or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being intimidating, racist, sexist, homophobic or defamatory. This is Cyberbullying and may be harassment or libel.
- When such comments exist online, for example, in the form of online posts, emails, tweets, videos, etc., you should not forward any such comments, as you will also be liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs, and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.

- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

In the event that any member of staff, student or parent/carer is found to be posting libelous or inflammatory comments on Facebook, for example, on the Mount Lourdes Facebook page, or any other social network sites in relation to the school, they will be reported to the appropriate 'report abuse' section of the network site. In serious cases the Board of Governors will also consider legal options to deal with any such misuse.

Safe use of USB/Memory Sticks

USB memory sticks have become increasingly popular because of their small physical size and large storage capacity. This has made them very convenient devices for transferring files from one place to another. However, these very features have introduced new information risks:

- Loss of information – a memory stick, like a computer, is susceptible to instant data loss or failure
- Potential breach of data confidentiality – if the memory stick is lost or stolen
- Physical loss – being so physically small the memory stick can be easily lost
- Corruption of data - if the memory stick is not removed from a computer properly.

In the majority of cases where data loss or corruption has occurred, it will be instantaneous and permanent.

Students should save working copies of their data on their computers in school or at home, and only use the memory stick for transportation of this data. Memory sticks should not be used to transport confidential, sensitive, or person-identifiable data.

The school can take no responsibility for the loss or corruption of data on students' memory sticks.

Netiquette for Online Lessons

It is important that you adhere to the same standards of behaviour online that you follow in school; any breaches of the rules will be dealt with according to our school's behavioural policy.

The following rules will help to establish an online platform that is safe, engaging and welcoming for all students:

- Check your device, camera, and microphone prior to the lesson.
- Use the Class Team set up by your teacher.
- If possible, use a quiet space in the house to minimise distractions for yourself.

- Your teacher will give you the option of turning your camera off if you wish, which you can do at this stage.
- If you choose to leave your camera on make sure you are dressed appropriately. You should not wear pyjamas / sleep wear during the session.
- Blur your background image for your own privacy and to minimise distractions for others.
- Your teacher will welcome you to the lesson and ask you to respond using your mic after which it can be muted to avoid a lot of background noise.
- The teacher may record the lesson so that it can be made available to students not present; however, he or she will make you aware of this in advance.
- You are not permitted to record any live lessons or any discussions taking place in breakout rooms.
- Aim to contribute to the lesson e.g. by answering questions, engaging where possible with the collaborative tools your teacher includes in the lesson, as this will help your teacher to assess your understanding.
- Use the Hand tool if you require to ask the teacher a question.
- Instructions given by the teacher during the lesson must be adhered to, just like in the classroom setting.
- Meet the deadlines set in the Assignment Tool.
- Inform the teacher if you are not able to attend the online lesson.
- When communicating with your class group either verbally through the audio facility or in the group chat always be mindful of the language you use. Do not use slang language.
- Students are not permitted to share recorded videos/lessons made by teachers within or outside of the class Team.
- Students must hang up at the end of the lesson once instructed to do so. The teacher must be the last person in the meeting to hang up.
- If you have any concerns after your lesson, contact your teacher.
- A disclosure or concern over any online forum will be followed up as it would be in school.

Remember when composing an email, you should:

- Only use your C2K email account.
- Add a subject to the email to help your teacher organise their correspondence.
- Please address the teacher at the start of the email by his or her name.
- Use appropriate formal language and avoid text language.
- Do not compose your email solely in capital letters.
- Sign off the email.

Useful websites

Safeguarding Board for Northern Ireland	https://www.safeguardingni.org/
UK Council for Child Internet Safety (UKCCIS);	http://www.education.gov.uk/ukccis/
Mental & Emotional wellbeing;	www.mindingyourhead.info
UK Safer Internet Centre;	http://www.saferinternet.org.uk/
Childnet International;	http://www.childnet.com/
SWGfL (South West Grid for Learning);	http://www.swgfl.org.uk/
ThinkU Know;	https://www.thinkuknow.co.uk/
NI Safer Schools	https://saferschoolsni.co.uk/
Online Safety Guides	https://www.internetmatters.org/issues/

Child Exploitation & Online Protection Centre (CEOP); http://ceop.police.uk/

Social Media Guides https://www.saferinternet.org.uk/advice-centre/social-media-guides

Links with other school policies:

- Addressing Bullying Behaviours Policy
- Positive Behaviour Management and Procedures Policy
- Pastoral Care Policy
- Child Protection Policy
- Relationships and Sexuality Education Policy.
- Bring Your Own Device Policy
- Mobile Phone and Electronic Device Policy