Acceptable Use of Internet and Email Policy

Ratified by the Board of Management on:

Date: 9th March 2020

(Amended on 28th April to include Protocols for Remote Learning)

Signature: _____________________________________

(Chairperson of the Board of Management)

Commenced: 2006
Date of last Review: 2020
Review due: 2022

Introduction

The aim of this Internet Acceptable Use Policy (AUP) is to ensure that pupils will benefit from the learning opportunities offered by the school's internet resources in a safe and effective manner.

Internet use and access is considered a school resource and privilege. If the school AUP is not adhered to this privilege may be withdrawn and appropriate sanctions will be imposed.

When using the internet pupils, parents and staff are expected to treat others with respect at all times. This includes:

- Not undertaking any actions that may bring the school into disrepute.
- Respecting the right to privacy of all other members of the school community.
- Respecting copyright and acknowledging creators when using online content and resources.

This Acceptable Use Policy applies to pupils who have access to and are users of the internet in Our Lady's School. It also applies to members of staff, volunteers, parents, carers and others who access the internet in Our Lady's School.

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

This policy and its implementation will be reviewed regularly by the following stakeholders:

- Board of Management, parents, teaching staff, and pupils.

This policy has been developed by a working group including: Principal, Deputy Principal, teachers, pupils, parents/guardians, and representatives of the Board of Management.

School Strategy

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet.

These strategies are as follows:

General Usage

- Internet sessions will always be supervised by a teacher.
- Software and/or equivalent systems will be filtered in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor pupils' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal electronic storage devices e.g. USB, in school requires a teacher's permission.
- Students will observe good "netiquette" (i.e., etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.
- Should serious online safety incidents take place, a member of the Senior Management Team should be informed.

Strategies to promote safer use of the internet

- Internet safety advice and support opportunities are provided to pupils in Our Lady's School through our SPHE, Pastoral Care lessons, IT classes and through initiatives and promotions that occur during the school term.
- Teachers will be provided with continuing professional development opportunities in the area of internet safety.

Content Filtering

Our Lady's School has chosen to implement the following level on content filtering on the school's Broadband Network:

- Level 5 - This level allows access to millions of websites including games and YouTube and allows access to personal websites category, and other similar types of websites, such as blogs but blocks access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

Pupils taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Web Browsing and Downloading

Pupils will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

Pupils will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Pupils will report accidental accessing of inappropriate materials in the classroom to their teacher.

Pupils will report accidental accessing of inappropriate materials in school but outside the classroom to their Year Head.

Pupils and staff will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Pupils will use the school's internet connection only for educational and career development activities.

Downloading by pupils of materials or images not relevant to their studies is not allowed.

Use of other 'unfiltered public wireless connections, such as mobile networks, is not allowed during the school day'.

Pupils will not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.

Email and Messaging

The use of personal email accounts is not allowed at Our Lady's School. The school designated email address should be used for all matters related to school.

Pupils should not use school email accounts to register for online services such as social networking services, apps, and games. The school email address adheres to a secure and managed system and therefore the use of the school email address for those issues aforementioned may result in the automated deactivation of the account and any work that is saved on said account.

Pupils should not under any circumstances share their email account login details with other pupils.

Pupils should be aware that email communications are monitored.

Pupils will not send any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Pupils should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils should avoid opening emails that appear suspicious. If in doubt, pupils should ask their teacher before opening emails from unknown senders.

Social Media

Staff and pupils must not use social media and the internet in any way to harass, insult, abuse or defame pupils, their family members, staff, other members of the Our Lady's School community.

Staff and pupils must not discuss personal information about pupils, staff and other members of the Our Lady's School community on social media.

Staff and pupils must not use school email addresses for setting up personal social media accounts or to communicate through such media.

Staff and pupils must not engage in activities involving social media which might bring Our Lady's School into disrepute.

Staff and pupils must not represent their personal views as those of Our Lady's School on any social medium.

Personal Devices

Pupils using their own technology in school should follow the rules set out in this agreement, in the same way as if they were using school equipment.

The following statements apply to the use of internet-enabled devices such as tablets, gaming devices, smart watches and digital music players in Our Lady's School :

- Pupils are only allowed to use personal internet-enabled devices during lessons with expressed permission from teaching staff. All use will be supervised by the teacher
- Pupils are not allowed to use personal internet-enabled devices during social time.
- Pupils may not use their devices to record, transmit or post photos/videos of other teachers, students unless they have been given permission by the teacher.
- Pupils are not allowed to have internet-enabled devices on their person during House or State Examinations. This includes any mobile, internet-enabled device such as a smart watch or mobile phone.
- Pupils/Guardians/Parents are responsible for their devices including any breakages, cost of repair or replacement
- The Principal, Deputy Principals reserve the right to inspect or monitor student mobile devices during school hours.
- Any such infractions will be dealt with under the procedures outlined in the Code of Positive Behaviour.

Images, Sound & Video

Care should be taken when taking photographic or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute or harm.

Sharing explicit images and in particular explicit images of pupils and/or minors is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other pupils automatically incurs suspension as a sanction.

At Our Lady's School pupils must not take, use, share, publish or distribute images of others without their permission.

Taking photos or videos on school grounds or when participating in school activities is only allowed with expressed permission from staff.

Written permission from parents or carers is obtained upon enrolment in order that photographs of pupils may be used for school purposes including, publishing of photographs on the school website.

Pupils must not share images, videos or other content online with the intention to harm another member of the school community regardless of whether this happens in school or outside.

Recording images, voice or phone calls without the express permission of the person being recorded, by any member of the school community, pupil, staff or parent runs contrary to the values of respect that we share at Our Lady’s School. Such actions that are deemed defamatory or that are intended to annoy, harass or intimidate another person may be subject to legal action.

Cyberbullying

When using the internet pupils, parents and staff are expected to treat others with respect at all times.

Engaging in online activities with the intention to harm, harass, or embarrass and another pupil or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.

Measures are taken by Our Lady's School to ensure that staff and pupils are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time (Dept. of Education 2013). This definition includes cyber-bullying even when it happens outside the school or at night.

Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and will be dealt with, as appropriate, in accordance with the school's Code of Positive Behaviour.

However, in the context of this policy, placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image, statement or any other form of intimidation or aggression can be viewed and/or repeated by other people will be regarded as bullying behaviour.

A single incident can have a serious effect on a pupil and may also constitute harassment which is legally prohibited in schools under equality legislation.

The prevention of cyber bullying is an integral part of the Anti-bullying Policy of our school.

School Websites

The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.

Webpages allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content.

The publication of student work will be coordinated by a teacher.

Personal student information including home address and contact details will not be published on Our Lady's School web pages.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and in extreme cases, suspension and expulsion. The school reserves the right to report any illegal activities to the appropriate authorities

Legislation

All members of the school community should familiarise themselves with the following legislation which relates, in part, to the use of the Internet:

Data Protection (Amendment) Acts 1988-2018
Child Trafficking and Pornography Act 1998
Interception Act 1993
Video Recordings Act 1989
The Data Protection Act 1988
General Data Protection Regulation (GDPR)

I agree to follow the school's Acceptable Use Policy on the use of the Internet. I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Student's Signature: ___________________________

Date: ____________________

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that

Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

Parent/Guardian : ___________________________

Date: ____________________

Attached Amendment to AUP Policy to include Remote Learning

GUIDELINES & PROTOCOLS FOR REMOTE LEARNING (Amendment to AUP)

Please be reminded that Our Lady's School Acceptable Use Policy and Code of Positive Behaviour remain in place for this period of remote learning and that users must engage in a responsible and appropriate manner at all times. It is essential that users review these policies and how they relate specifically to online behaviour when using technology for education.

During the current school closure, the school approved educational platform GOOGLE - G-SUITE for Education is in use to support and facilitate teaching and learning. All of the protocols contained in the aforementioned policies are relevant to the use of these apps for online learning and must be observed in all communications between students and teachers.

School GMAIL accounts are set up for all student-teacher-class contact. Personal email addresses are not permitted and should not be used. Please note that individual emails from students to teachers should be sent during normal school working hours with queries/submissions that relate to subject work only.

STUDENTS & PARENTS

Students are reminded of their responsibilities in line with the school's Code of Positive Behaviour and Acceptable Use Policy. Students and parents should take time to familiarise themselves with both policies and engage with them in a positive manner.

- We ask students to be mindful of email etiquette as distinct from online communication with peers. For example, address the relevant teacher at the beginning of email, maintain a polite tone throughout, and sign off as appropriate.
- The use of social media applications or setting up of private groups (e.g WhatsApp; Facebook, Snapchat, Instagram) for class or student-teacher communication is strictly prohibited.
- The use of subject content-based videos and images including voiceovers may be used by teachers and students to share and submit class work.
- The use of live cameras and mics during a lesson by students is only permitted as instructed by your teacher.
- Live chat may also be used for classes as part of the Google G-Suite for education applications. These functions are to be used only with the express permission and instruction of the teacher.
- Please enter the lesson with the microphone muted and listen for the teacher's instruction. You may have your camera turned off at your discretion. However, if a teacher requests you to turn off your camera you must do so immediately.
- If choosing to have your camera on then you must ensure you are suitably dressed and in a quiet space with a suitable backdrop.
- Students are advised to follow their daily timetable to maintain a structured approach to learning. Students are required to check their GMAIL ACCOUNT each day to collect assigned work and instructions from various subject teachers. It is important for learning that students engage with the set tasks and activities to the best of their ability in current circumstances; and that they submit work on completion as advised by their subject teachers. Parents are to notify their daughter's Year Head if she is unable to partake in remote learning due to illness/family reasons. Students are encouraged to approach their teacher for assistance/extension if a particular deadline is causing difficulty.
- Students are not permitted to record or distribute any online lessons without the express consent of the teacher. Teachers may record the delivery of the lesson in order to post the lesson on their Google Classroom for students to reference at a later stage. The teacher will always inform students that the class is to be recorded and ask students to mute mics and to turn off their cameras if they wish. If a student wishes to rescind their consent then they have that right and should articulate it clearly to the teacher.
- If work is assigned using Google Classroom, students should take extra care to submit via Classroom also rather than mailing it to the teacher's school email address.

- As student internet access cannot be supervised by teachers during this period of school closure, student personal responsibility is essential and/or parental/guardian monitoring where possible.
- Parents should ensure adequate cyber security systems such as anti-virus programmes are in place and updated.
- Parents should take time to explain online safety and etiquette to their daughters. Phishing, scamming and other online criminality are prevalent and every effort should be made by both parent and student to fully understand measures to protect themselves and their information whilst online. Please visit www.webwise.ie for assistance with such matters.
- If students have any queries regarding remote learning or require assistance with accessing Gmail or other approved educational apps - please email remotelearning@olschool.ie .

Please contact a member of your relevant care team if there are any other issues affecting your ability to engage with remote learning.

STAFF

Staff are permitted to use only their school email address in any correspondence with students. The school educational platform G-Suite for Education is a protected domain and should be used as the primary tool for remote teaching and learning.
School emails are filtered through the school's domain which is a managed and secure system. Any misuse of school emails may result in the deactivation of the account and the loss of any saved information.
In exceptional circumstances such as data breach investigations and child protection investigations the email account may be examined.
The school email account must only be used for school based business.
Teachers leaving the staff, through retirement or resignation, will have their email accounts deactivated within 2 months of their departure.
Online, live classes are encouraged daily with the following precautions:

- Online classes should only take place using Google Hangout/Meet. There are functions on this platform, controlled by the administrator that ensures certain safeties for students and staff e.g. students are unable to record. Non-approved platforms, such as Zoom, should not be used.
- If recording the instruction segment of the live lesson to post on the Google Classroom later for students who may not have had access at the time of the live lesson, should be done so with the following caveats: Students microphones and cameras should be switched off. Students' right not to consent should be strictly abided by.
- Both teachers and students should wear appropriate attire.
- Both teachers and students should be aware of their background and environment if using the camera option.
- Teachers should be extremely careful when presenting to not expose sensitive information on other open tabs on their computer.
- If presenting during the live class all pop-up notifications should be turned off, especially for their school gmail account.
- Sensitive conversations that may have been appropriate before or after class in a controlled, safe environment should not take place online unless deemed extremely necessary. Contact, by phone, through communication with the parent is a safer option.
- Classroom rules extend to online classrooms. Any misbehaviour or absenteeism should be recorded and Year Heads made aware.
- Students should be reminded of their responsibilities in line with the Code of Positive Behaviour and the Acceptable Use Policy.
- Child protection protocols extend to online classes. Appropriate recording and communication of any concerns should be made in line with the school's Child Protection Policy.
- Teacher's should make themselves aware of the GDPR and Cyber Security responsibilities outlined below.

MINIMISING RISK WHEN TEACHING REMOTELY

GDPR - Staff working from home

In light of the Covid19 situation and in addition to advice on good cyber security practices the following precautions should be taken to minimise risk when teaching remotely.

With regard to hard copy documents that contain personal data, staff are reminded of the following:
- where possible, keep a written record of which records and files have been taken home, in order to maintain good data access and governance practices;
- to the greatest extent possible avoid printing material; if printing is necessary then ensure that documents are stored and handled in line with their sensitivity;
- take appropriate steps to ensure the security and confidentiality of paper records, for example, by keeping them locked in a filing cabinet or drawer when not in use;
- take extra care when dealing with special categories of personal data (e.g. SEN, health data), and only remove such records from a secure location where strictly necessary;
- make sure you dispose of documents securely (e.g. shredding) when hard copies are no longer needed.

Data Breach when working from home

Staff should be aware that if a data breach were to occur, school management will need to be alerted and informed of the facts without undue delay. The school, as data controller, is required to strictly adhere to the regulations concerning data breach notifications and communications, regardless of whether the data breach occurs inside or outside the school. This includes a 72 hour reporting window to the Data Protection Commission irrespective of working days.

Good cyber-hygiene practice within the home

Staff using their own devices

If personal devices are being used by staff, compliance with the following checklist will help to reduce risk:
- device access is controlled by a strong password, passcode or PIN
- anti-virus software is installed and up-to-date
- operating system (Windows or Mac) is up-to-date
- device firewall is enabled
- device storage is encrypted
- two-factor authentication (2FA) is activated for accounts that allow access to school data.
- default passwords have been changed on software or devices – including home Wi-Fi 1
- no storage of school data on personal device is allowed (if this is unavoidable then a strong password should be applied to such files).

All staff should be aware that good data security practices also require that:
- great care is needed when any personal data is stored on a local device
- device screens are not visible to others when personal data is being accessed
- screen savers automatically activate when the device is not in use
- care is exercised around the security and use of any USB devices.

Cybersecurity, The NCSC reports that it has observed an increase in phishing and malware campaigns exploiting the COVID19 pandemic. Email is the primary channel for cyber-attacks. A typical phishing email contains a lure to induce the recipient to activate the “payload” (usually by clicking on an attachment or a link). This usually links to malware or sites designed to install ransomware, steal credentials or banking details, or enable further remote access by the attackers. Phishing emails can be convincing to even seasoned IT users and emails related to COVID-19 often try to create a sense of urgency to rush people into making a mistake. Phishing emails might be targeted at staff, such as happened with a recent data breach at the Teaching Council, or at other recipients such as parents. For example, in the UK, the Department for Education has recently highlighted a scam email asking parents of children eligible for free school meals for their bank details, so that their child could still receive meals during school closures. When it comes to prevention there are many sources of advice available for example, Staying Safe Online during a Pandemic.

A reminder that all communications should use "work" email addresses rather than personal emails.

In terms of communications between staff, best practice is that staff should minimise any online discussions that include special category data (e.g. data about SEN issues) that relates to identifiable students. Often these communications are best handled through direct telephone conversation.