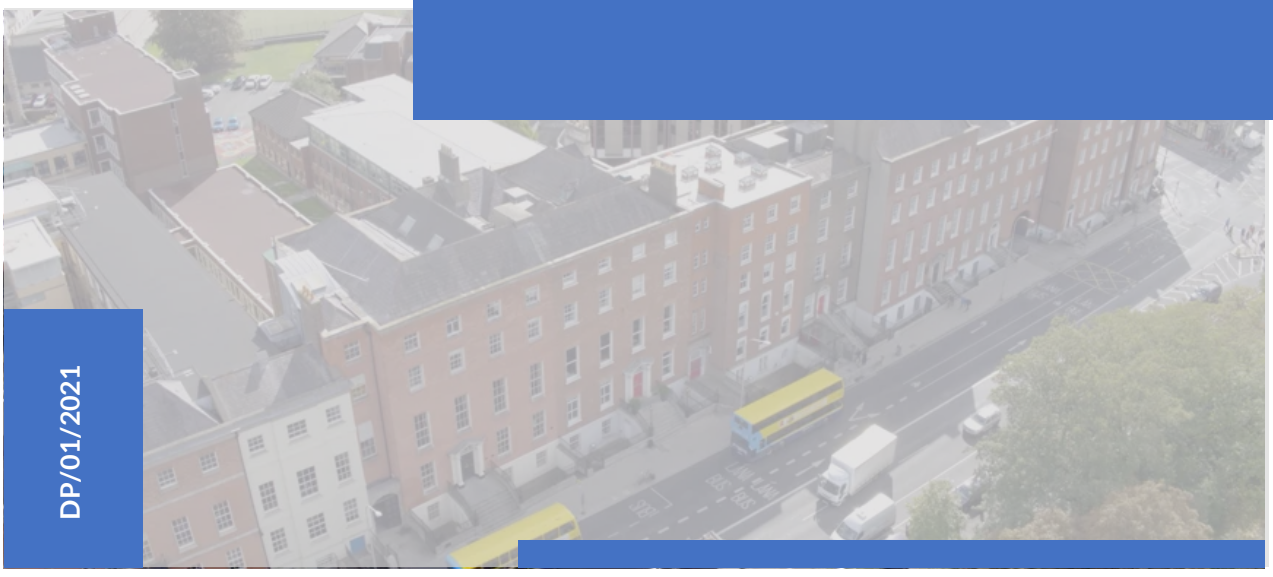
Acceptable Use Policy (Student)

The following Acceptable Use Policy has been developed to reflect the school's commitment to the correct and proper use of its ICT resources.

01 661 8179

53/55 St. Stephen's Green,
Dublin.

info@loretothegreen.ie



DP/01/2021

APPROVED BY
Board of Management

DATE ISSUED
17 January 2022

Student Acceptable Use Policy

Document Title

Student Acceptable Use Policy

Revisions

No.	Status	Author(s)	Approved By	Office	Issue Date
Rev 01	Release	Ark www.arkservices.ie	Ark	Cork	December 2021

Circulation

Position	Office	Issue Date	Method
Senior Management	Loreto College	December 2021	Email
Board of Management	Loreto College	December 2021	Email
Students	Loreto College	December 2021	Email

Table of Contents

Acceptable Use Policy

Loreto College (School) is committed to the correct and proper use of its ICT resources in support of its teaching & learning functions.

Purpose
Loreto College has invested significantly in the provision of technologies to aid teaching and learning as well as facilitate remote teaching and learning (where needed) in the school. Loreto College (School) is committed to the correct and proper use of its ICT resources.

The inappropriate use of information and communication technology (ICT) resources could expose the school to risks including virus and malicious software attacks, theft and unauthorised disclosure of information, disruption of network systems and / or litigation.

The purpose of this policy is to provide students as users of its ICT resources with clear guidance on the appropriate, safe and legal way in which they can make use of the school's ICT resources.

Scope
This policy represents the school's position and takes precedence over all other relevant policies. The policy applies to:

- All ICT resources provided by the school.
- All students as users of the school's ICT resources.
- All use (both personal & school related) of the school's ICT resources.
- All connections to (locally or remotely) the school network Domains (LAN/WAN/Wi-Fi).
- All connections made to external networks through the school network.

General Principles
The acceptable use of the school's ICT resources is based on the following principles:

- All ICT resources and related information remain the property of the school.
- Users must ensure that they use ICT resources at all times in a manner which is lawful, ethical and efficient.
- Users must respect the ICT devices and equipment provided for their use and take all reasonable steps to prevent damage, loss or misplacement.
- Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.
- Users must respect the integrity and security of the school's ICT resources.

Breaches of this policy may be treated as a matter for discipline. Depending on the seriousness of the breach this will be dealt with by the Principal in accordance with the School's Code of Behaviour. For breaches which do not warrant such action, those involved will be advised of the issue and given a reasonable opportunity to put it right.

Board of Management of Loreto College approved the Acceptable Use Policy.

_____ _____
Chairperson **Date**

1. Objectives

- Protect and maintain the integrity of the ICT Resources and make communications reliable.
- Support teaching and learning.
- Implement best practice in the appropriate use of ICT Resources.
- Ensure that users engage only in the appropriate uses of ICT Resources to meet the needs of staff and students.

2. Responsibilities – Students

Our entire school community have a role in implementing the Acceptable Use Policy.

Students are required:

- To agree to exhibit responsible behaviour in the use of all ICT resources as set out in the Acceptable Use Policy (Students).
- To take personal responsibility for not accessing inappropriate material on the internet.
- To accept that Loreto College is not responsible for materials, or information of any kind, placed on the network by third parties.

3. Responsibilities – Parents / Guardians

Our entire school community have a role in implementing the Acceptable Use Policy.

Parents are required:

- To support the school's Acceptable Use Policy.
- To become familiar with the school's Acceptable Use Policy and to discuss it with their child.
- To accept responsibility for supervision, if and when a student's use of email and the internet is not in a school setting.

4. ICT Department

- The ICT Department is made up of the Director of eLearning, ICT Support and the Student Enrichment Officer.
- The ICT Department will coordinate and support the technical implementation of the policy on an ongoing basis.

5. Routine Monitoring

The school reserves the right to routinely monitor, log, audit and record any and all use of its ICT resources for the purposes including:

- Helping to trace and resolve technical faults.
- Protecting and maintaining network and system security.
- Maintaining system performance and availability.
- Ensuring the privacy and integrity of information stored on the network.
- Investigating actual and suspected security incidents.
- Preventing, detecting and minimising inappropriate use.
- Protecting the rights and property of the school, its staff, students and wider school community.
- Ensuring compliance with other school policies, current legislation and applicable regulations.

6. User Accounts & Passwords

Where appropriate, individual students will be granted access to the school's ICT resources.

- Each student will be assigned an individual username and password set which they can use to access a particular ICT resource.
- Each student is responsible for all activities performed on any ICT device, or software application while logged in under their own individual account and password.
- Students must ensure all passwords assigned to them are kept secure.
- Students should not use the same password for their personal accounts i.e. social media, as their school supplied accounts.
- Passwords must contain a minimum of 8-12 characters including a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: ", £, $, %, ^, &, *, @, #, ?, !, €).
- Students who suspect their password is known by others must change their password immediately.

7. Wi-fi Use

Wi-fi Use

- Internet access is provided by PDST NCTE (School-Filtered Broadband).
- The school's Wi-Fi is available to all students where appropriate.
- Appropriate technical measures are in place for to safeguard student's use of Wi-Fi.
- At all times, students must use their school login details and their own school supplied cloud.
- Internet sessions will be supervised by a teacher in class, where possible.
- Downloading of materials or images by students, which is not relevant to their studies, is in direct breach of this Acceptable Use Policy.
- Students must not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise explicit or objectionable materials.
- Students must report accidental accessing of inappropriate materials in accordance with school procedures.
- Students must log out of their own accounts at the end of each Internet session when using a common device.
- Students are not permitted to access the school accounts of other students.
- In the event where a student accesses a school device and finds another student or member of staff has not logged out, the person accessing the device must log the other person out before proceeding to use the device.
- It is not permitted for students to delete the work or files of other students from folders on the school network.
- It is not permitted for any student to attempt any act of hacking or other form of sabotage that could compromise the security of the school's network. Any such action will result in a school sanction being imposed.

8. ICT Devices & Equipment

All ICT devices and equipment are purchased through the agreed channels.

- All ICT devices and equipment provided to students remain the property of the school.
- ICT devices purchased by the student i.e. iPads, will be provisioned and set up for operation on school networks. The school will be responsible for the software provision in relation to school business and the student will be responsible for iPad itself.
- Students must not remove or borrow school ICT devices or equipment without the authorisation of the ICT Department.
- The physical security of any school ICT devices and equipment borrowed is the responsibility of the borrower and the ICT devices and equipment must be returned by the borrower before they leave the school or, at the request of the ICT Department.
- Students must take due care when using school ICT devices and equipment and take reasonable steps to ensure that no damage is caused to the ICT device or equipment.
- Students must take all reasonable steps to ensure that the device is protected against loss or theft.
- All school supplied devices will be set up with a password / pin code / swipe gesture to gain access.
- Passwords used to access school ICT devices must not be written down on the device or stored with or near the device.
- Students must not alter the hardware or software configuration of any school ICT device or equipment without the prior authorisation of the ICT Department.
- Students are not permitted to consume food or liquids whilst using school supplied ICT devices or equipment.
- Student must report all damaged, lost or stolen school ICT devices and equipment to their Class Teacher.
- Where relevant, ICT Equipment must be returned by students before they leave the school. Once notified, the ICT Department will then disable access to ICT resources within 1 month.
- The school reserves the right to remove any ICT devices and equipment from the network at any time, for reasons including but not limited to (1) noncompliance with school policies, (2) the ICT device or equipment does not meet approved specification and standard, or (3) the ICT device or equipment is deemed to be interfering with the operation of the network.

9. Access to School Network

Access to school network domains and network resources is controlled and managed by the ICT Department.

- Access rights and privileges to the school network domains and network resources will be allocated based on the specific requirement of each student through the ICT Department.
- Access to school network domains will be controlled by the use of individual user accounts.
- Students must not:
    - Connect or disconnect any school ICT devices, equipment or removable storage devices to or from a school network domain without the prior authorisation of the ICT Department.
    - Connect any school ICT devices and equipment, laptop or smart device to an external network without the prior authorisation of the ICT Department.
    - Connect any ICT devices and equipment, laptop, smart device, mobile phone device or removable storage device which is their personal property and is not owned or leased by the school to a school network domain without the prior authorisation of the ICT Department.

10. Information Storage

- Photographic, video and audio recordings which are taken as part of school business must be transferred from the recording device (i.e. digital camera, video camera, mobile phone, tape recorder etc) onto a school network server or cloud as soon as is reasonably practicable.

11. Students Use of Technology - General

- Internet sessions will be supervised by a teacher, where possible.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' Internet usage.
- The use of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of digital storage media (e.g. Cloud storage, memory sticks/cards, personal USBs, CDROMs etc.) in school requires a teacher's permission.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- Students are forbidden from opening apps in class or going online, unless instructed to do so, and only for the purposes instructed by a teacher.
- Students will not use school supplied ICT resources for personal reasons.
- School email accounts should not be used to sign up to other non-educational apps or websites.

12. Use of Email

- Students will use their school email account for educational use only.
- Students will use school supplied school email accounts for communications with teachers (using the teacher's school email account).
- Students will not send any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses, telephone/mobile phone numbers or pictures.

13. Protocol for Remote Learning & Live Classes

Should the school need to revert to a remote teaching / learning approach.

- Each teacher and student has been assigned an individual account, username and password for G-suite for Education which they can use for remote teaching and learning.
- Only the individual to whom the account was assigned is permitted to use such account i.e. Each school account is for the sole use of the teacher / student only.
- The school will only correspond with the account holder, and should there be a breach of this policy, the school will suspend the account indefinitely.
- Only teachers are permitted to record live classes.
- Students are expected to conduct themselves with respect for both the teacher and their classmates.

When broadcasting classes live, staff should be conscious of the two options available:

  - Option 1: Choose a window to share that specific program and its content, (preferable option as it restricts the viewers visibility to one dedicated program).
  - Option 2: Select Desktop to share everything on your screen (which can lead to inadvertent sharing of information).

Take care to not display any personal data i.e. close down other applications, email or documents which contain personal data prior to showing your screen / recording classes.

14. Internet Use

- Students will use the Internet for educational purposes only.
- Internet sessions will be supervised by a teacher, where possible.
- Internet access is provided by PDST NCTE (School-Filtered Broadband) for teaching and learning.
- Appropriate school Wi-Fi is available to all students.
- No other networks/personal data (3G, 4G, Personal Hotspots etc.) may be used by students while on school grounds or as part of a school activity, unless under the direct instruction / supervision of a teacher.
- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise explicit or objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures. Students should retain their usernames and password securely.
- Students will never arrange a face-to-face meeting with someone they only know through emails or other online communication without the permission of their teacher.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement). Students will be required to exercise care and attention in citing sources, references, photos/images and to acknowledge copyright if some material is used in their work. When downloading material from the Internet, students will take reasonable care to ensure that the material is from safe sources, copyright-free (where possible) and referenced appropriately.
- Students will never disclose or publicise personal information in relation to themselves or others.
- Students should note that any usage, including distributing or receiving information, school related or personal, may be monitored for unusual activity, security and/or network management reasons.
- School Devices will be available to students. At all times, students must use their school login details and their own storage area on the school supplied cloud.
- It is not permitted for students to delete the work or files of other students from folders on the school network.
- It is not permitted for any student to attempt any act of hacking or other form of sabotage that could compromise the security of the school's network and digital data. Any such action will result in a serious sanction being imposed, including the option to suspend or expel the student involved.
- Students must log out of their own accounts at the end of each Internet session. Students are not permitted to access the school accounts of other students. In the event where a student accesses a school device and finds another student has not logged out, the student accessing the device must log the other student out before proceeding to use the device. The student should also inform the relevant teacher.

15. Unacceptable Use

The following list should not be seen as exhaustive. The school has the final decision on deciding what constitutes excessive personal use. The school will refer any use of its ICT resources for illegal activities to the Gardai.

- To knowingly misrepresent the school.
- To store or transfer confidential or restricted information on a USB memory stick.
- To create, view, download, host or transmit material of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. material is defined as information (irrespective of format), images, video clips, audio recordings etc.
- To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others.
- To retrieve, create, host or transmit material which is defamatory.
- Any activity that would infringe intellectual property rights (e.g. unlicenced installation, distribution or copying of copyrighted material).
- For any activity that would compromise the privacy of others.
- For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the school or others.
- Any activity that would deliberately cause the corruption or destruction of data belonging to the school or others.
- Any activity that would intentionally compromise the security of the school's ICT resources, including the confidentiality and integrity of information and availability of ICT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection).
- The installation and use of software or hardware which could be used to probe or hack the school ICT security controls.
- For the installation and use of software or hardware which could be used for the unauthorised monitoring of electronic communications within the school or elsewhere.
- Creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements.
- Any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.