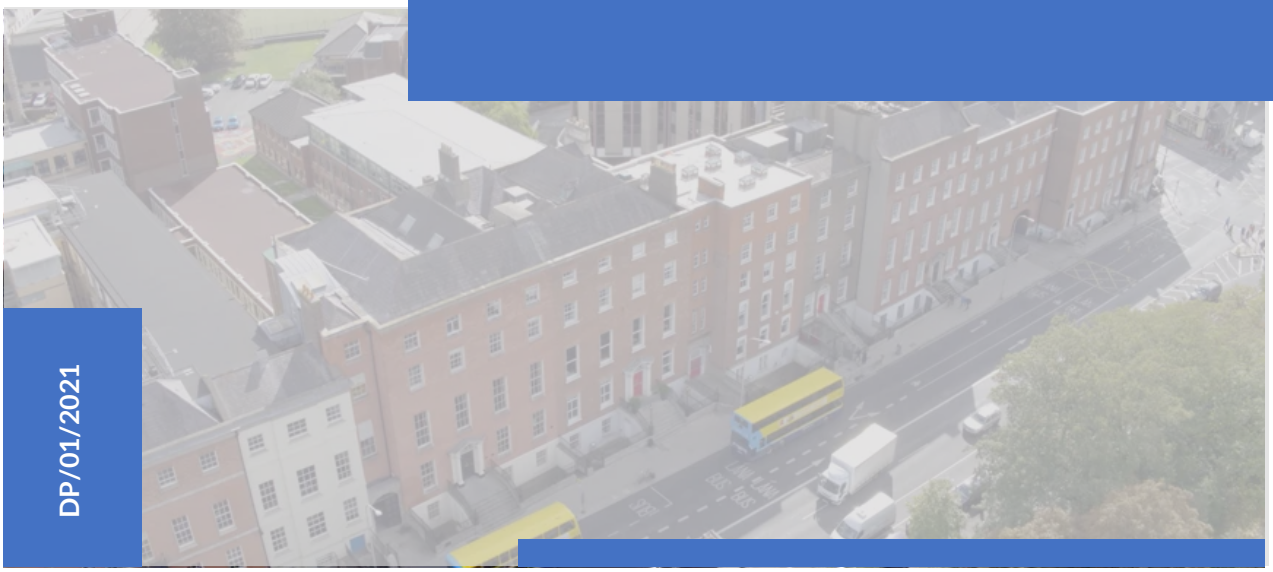
Acceptable Use Policy (Staff)

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

Staff Acceptable Use Policy

Document Title
Staff 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
Staff	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.
- Provide for the professional development needs of staff.

2. Responsibilities – Board of Management

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

- The Board of Management will approve the policy and ensure its development and evaluation.
- As new technologies are developed that may prove valuable to our teaching and learning goals, to evaluate and provide access to them if necessary.
- To consider reports from the Principal and the ICT Department on the implementation of the policy.

3. Responsibilities – Senior Leadership Team

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

- The Senior Leadership Team will be responsible for the dissemination of the policy.
- To oversee implementation of the policy.
- To establish structures and procedures for the implementation of the Acceptable Use Policy.
- To provide all staff - including teachers, students resource teachers, supply staff, special needs assistants and administrative staff with the school's Acceptable Use Policy.
- To notify all parties when the policy has been updated.
- To provide training for staff in the appropriate and responsible use of ICT Resources.
- To ensure that users understand that failure to adhere to this Acceptable Use Policy will result in the loss of privilege and/or disciplinary action.
- To monitor the implementation of the policy.

4. Responsibilities – 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 with staff on an ongoing basis. Responsibilities include:

- Provide input on the implementation of the policy.
- Establish practices and procedures for the implementation of the Acceptable Use Policy.
- Maintain a list of "Approved ICT Resources".
- Where the AUP has been breached, report the breach to the Principal.
- Monitor the implementation of the policy and provide feedback to the Principal where relevant.
- Only access administrator accounts via their school supplied trusted device.
- When providing support to colleagues on their own personal device, via the relevant support account (not admin account) the following measures must be in place:
    - Such devices must be secured by a password or a biometric access control (e.g., fingerprint scanner or facial recognition).
    - Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed.
    - Such devices must be configured so that they are automatically locked after being left idle for a set time e.g., 1 minute.
    - 2 Factor Authentication must be enabled and used for apps used.
    - Such devices must not be used by family members or other persons. Passwords to such devices must be kept confidential and must not be shared with family members or third parties.
    - Care must be taken to avoid using such devices in a manner which could pose a risk to confidentiality, or personal data whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g., coffee shops or airports), or otherwise.
    - In the event that such a device is lost or stolen, or is suspected of having been lost or stolen, the Principal must be informed as soon as possible so that such steps as may be appropriate may taken to mitigate the consequences of the loss.
    - Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
    - If such a device needs to be repaired, appropriate steps must be taken to ensure that confidential information or personal data cannot be seen or copied by the repairer.
    - In the event that such a device needs to be disposed of, confidential material must be destroyed or wiped using a recognised method to put the data beyond recovery, to the satisfaction of Loreto College.

5. Responsibilities – Non Teaching Staff

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

Non-teaching Staff are required:

- To accept the terms of the Acceptable Use Policy before using any ICT Resource in the school.
- To monitor their use of ICT resources in line with this policy.
- To immediately report any violation of the Acceptable Use Policy to the ICT Department.

6. Responsibilities – Teaching Staff

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

Teaching Staff are required:

- To accept the terms of the Acceptable Use Policy before using any ICT Resource in the school.
- To instruct students in the appropriate use of ICT resources as set out in the Acceptable Use Policy (Students).
- To monitor the use of ICT resources.
- To record any violations of the Acceptable Use Policy and inform the Senior Leadership Team.
- Impose appropriate sanctions for violations of this policy.
- To report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.

7. Responsibilities – Administration Staff

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

Administration Staff are required:

- To accept the terms of the Acceptable Use Policy before using any ICT Resource in the school.
- To monitor their use of ICT resources in line with this policy.
- To immediately report any violation of the Acceptable Use Policy to the ICT Department.

8. 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.

9. 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.

10. The Child Trafficking & Pornography Act 1998

The sharing or storing of explicit images is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.

- Every student in the school has a right to a safe learning environment in school at all times, free from risk of exploitation.
- The school has a duty of care to students under various legislation including but not limited to the Safety, Health & Welfare at Work Act 2005 as well as the Child Trafficking And Pornography Act 1998 and any other related legislation.
- The Board of Management reserve the right to contact the Gardai should there be a strong suspicion of a member of staff acting illegally using school ICT Resources.

11. Approved ICT Resources

Approved ICT Resources are technologies that the school has approved for use by staff and students in the context of teaching and learning. From time to time this list may be updated to reflect changes in how Loreto College do things or changing circumstances outside our control.

- The ICT Department will maintain a list of "Approved ICT Resources".
- ICT resources must be vetted through the ICT Department prior to purchase / subscription / licencing of these ICT resources.
- A record of decisions will also be maintained to demonstrate which ICT resources were approved (or not).

12. Routine Monitoring

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

Whilst the school does not routinely monitor an individual's use of its ICT resources it reserves the right to do so when a breach of its policies or illegal activity is suspected. The monitoring may include, but will not be limited to individual login sessions, details of information management systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, and the content of electronic communications.

Loreto College will at all times seek to act in a fair manner and respect the individual user's right for the privacy of their personal information under the Data Protection Act 2018.

Information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly in the users interest to do so or it reveals activity that the school could not be reasonably expected to ignore, for example a user found to be viewing, downloading or forwarding pornography must be reported to Gardai.

Individual monitoring reports will only be accessible to the appropriate authorised personnel and will be deleted when they are no longer required.

13. ICT Devices & Equipment

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

- Purchases of ICT equipment and resources must be vetted through the ICT department.
- All ICT devices and equipment provided to staff remain the property of the school.
- ICT devices and equipment will be registered on an Asset Register.
- ICT Devices will be provisioned with appropriate technical measures to safeguard personal data i.e. encryption of hard drives.
- School supplied ICT devices are then known as “trusted devices”.
- Staff 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 employment of the school or, at the request of the ICT Department.
- Shared devices for student use (Classroom Windows Laptops) will not be configured with a password. Class teachers are responsible for instructing students to log out of their device at the end of class.
- Staff must not alter the hardware or software configuration of any school ICT device or equipment without the prior authorisation of the ICT Department.
- Staff 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.
- Staff are not permitted to consume food or liquids whilst using ICT devices or equipment.
- Staff must report all damaged, lost or stolen school ICT devices and equipment to the ICT Department.
- ICT equipment must be returned by staff before they leave the employment of 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.
- The school reserves the right to alter, modify or reconfigure any ICT devices i.e. push patches, updates or removal of software at any time.

Old and obsolete school ICT devices and equipment will be recycled in accordance with the requirements of the European Waste Electrical and Electronic Equipment (WEEE) Directive. Staff must notify the ICT Department of old and obsolete ICT devices and equipment and the ICT Department will facilitate the collection and disposal of the devices and equipment.

14. Mobile Devices

Staff must ensure that school devices and smart devices provided to them are protected at all times.

- Staff must ensure that school supplied trusted mobile devices provided are protected at all times.
- Staff must take all reasonable steps to ensure that no damage is caused to the device and that the device is protected against loss or theft.
- School devices will only be issued to staff who have signed acknowledgement and acceptance of the Acceptable Use Policy.
- All school iPads are registered with the ICT Department through Apple School Manager so that they can be routed through the school network infrastructure and managed securely.
- All school supplied trusted devices provided to staff will be set up with a password / biometric / pin code / swipe gesture to gain access.
- Passwords used to access these trusted devices must not be written down on the device or stored with or near the device.
- When traveling by car, trusted mobile devices should be stored securely out of sight when not in use. Staff are advised to avoid storing these devices unattended in the boot of a car overnight.
- The use of school smart devices within a car must at all times be carried out in accordance with the Road Traffic Act 2006.
- When traveling by taxi, train or plane school laptops, mobile computer devices and smart devices should be kept close to hand at all times. Avoid placing the devices in locations where they could easily be forgotten or left behind (i.e. in overhead racks or boots of taxis).
- When using a trusted mobile device, staff need to take precautions to ensure the information on the device screen cannot be viewed by others. In addition, Staff are advised to connect to Wi-Fi networks that are secure i.e. password protected.
- Staff must ensure that all trusted mobile devices provided to them are not accessed (including internet access) by persons who are not school staff (i.e. friends, family members and others etc).

15. Computer & Peripherals

Staff should be conscious of the use of computers and peripherals in the day to day operation of the school.

- Staff should operate a clear screen policy when connected to the projector i.e. all applications displaying personal data should be closed.
- Staff are encouraged to use "Freeze" or "Blank screen mode" when accessing personal data whilst connected to the projector.
- Staff must disconnect from the projector when leaving the class.
- Staff must log off or 'lock' their school computer (using *Ctrl+Alt+Delete* keys on Windows laptops) when they have to leave it unattended for any period of time and at the end of the each working day.
- Where practical staff should operate a clear desk policy and clear their desks of all confidential and restricted personal data (irrespective of the format) at the end of each working day or when leaving the school for a major part of the day.
- Where possible, printers, scanners and photocopiers which are used to regularly print, scan or copy confidential or restricted information should be located within areas which are not accessible by the general public.

16. Personal Use

Loreto College's ICT resources are used primarily for school business. However at the discretion of Principal occasional personal use may be permitted by a member of staff provided it:

- Does not involve the use of personal data collected by the school for teaching and learning purposes.
- Is not excessive.
- Does not take priority over their school work responsibilities.
- Does not interfere with the performance and work of the user, other staff or the school.
- Does not incur unwarranted expense or liability for the school.
- Does not have a negative impact on the school in any way.
- Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit.
- Is lawful and complies with this policy and all other relevant school policies.

The school has the final decision on deciding what constitutes excessive personal use. The school does not accept liability for any fraud or theft that results from a user's personal use of the school's ICT resources.

17. Wi-fi Use

Wi-fi Use

- School supplied trusted ICT Resources and devices will be available to staff.
- At all times, staff must use their school login details and their own school supplied trusted cloud.
- Internet access is provided by PDST NCTE (School-Filtered Broadband).
- The school's Wi-Fi is available to all staff.
- The Wi-Fi is protected using Sonic Wall (Firewall) and to help ensure student and data safety.
- Downloading of materials or images by staff, which is not relevant to teaching and learning, is in direct breach of this Acceptable Use Policy.
- Staff must not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise explicit or objectionable materials.
- Staff must report accidental accessing of inappropriate materials in accordance with school procedures.
- Staff must log out of their own accounts at the end of each Internet session when using a common device.
- It is strictly forbidden for staff to delete the work or files of other staff from folders on the school network.
- It is strictly forbidden for any member of staff 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.

18. Software & Electronic Media

Each member of staff is responsible for making use of software and electronic media in accordance with the Irish *Copyright and Related Rights Act 2000* and software licensing agreements. An "Approved ICT Resources" List is maintained by the ICT Coordinator. Staff should consult the ICT Department before purchasing downloading, accessing or using any 3rd party software in connection with school business.

- Only software which has the correct and proper licence may be installed and used within the school.
- Software and mobile apps must only be downloaded and installed on school supplied trusted devices where there is a valid school reason, and the software can add value to teaching and learning in the school.
- All software and electronic media developed and purchased on behalf the school remains the property of the school and must not be used, copied, distributed or borrowed without the authorisation of the ICT Department.
- The school reserves the right to remove software at any time, for reasons including but not limited to:
    - Non-compliance with school policies.
    - The software is not properly licenced.
    - The software is found to have a negative impact on the performance of the school network, systems or equipment.

19. Confidentiality & Privacy

The school as a Data Controller is legally required under the Data Protection Act 2018 to ensure the security and confidentiality of all personal data it processes.

- Staff must respect the privacy and confidentiality of personal data at all times.
- Staff must not access personal data or management information systems unless they have a valid school related reason to do so, or they have been granted permission by Senior Management and / or the ICT Department.
- Staff must not remove any confidential or restricted personal data (irrespective of format) from the school without the authorisation of the Principal.
- Confidential and restricted personal data must only be discussed or shared with others on a strict "need to know" basis.
- Confidential and restricted personal data must only be discussed or shared with other staff or staff of a government funded agency in accordance with the school's Data Protection Policy.
- Confidential and restricted personal data must only be released / disclosed to other government agencies and departments in accordance with the relevant legislation where there is a valid written request.
- Where it is necessary to release or disclose confidential or restricted personal data to third parties, only the minimum amount of data should be released as is absolutely necessary for a given function to be carried out.
- Appropriate technical & organizational measures should be adopted to ensure that data is kept secure i.e. password protecting documents before emailing.
- Confidential or restricted personal data (irrespective of the format) must not be copied, renamed, deleted or modified without the authorisation of the Principal. This includes personal data on storage devices and information in transit.
- Personal data belonging to school staff or students must not be used for presentations, training or testing purposes unless it has first been anonymised or pseudonymised (coded). Otherwise the explicit consent of the school and the individual (as a Data Subject) is required from the parent / guardian of the student (where students are under 18 years).
- Staff must ensure that all software applications or network access provided to them are not accessed (including internet access) by persons who are not school Staff (i.e. friends, family members and others etc).

Please refer to the school's Data Protection Policy which provides clear guidance regarding the expected use of personal data in the school. The policy is available from the Principal.

20. User Accounts & Passwords

Where appropriate individual users will be granted access to the school's ICT resources which are necessary for them to perform a specific task in the school. Please refer to the school's Data Protection Policy which provides clear guidance regarding the use of data in the school. This policy is available from the school website.

- Each authorised user will be assigned an individual user access account name and password set which they can use to access a particular ICT resource.
- Accounts will be provisioned on a "least privileged access" basis i.e., a user is given the minimum levels of access or permissions needed to perform his/her function.
- Staff are not permitted to access the school accounts of other staff.
- Should a member of staff access a school device and finds another member of staff has not logged out, the person accessing the device must log the other person out before proceeding to use the device.
- Each user is responsible for all activities performed on any ICT device, management information system or software application while logged in under their own individual access account and password.
- Staff must ensure all passwords assigned to them are kept secure. Staff must not write down their password(s) on or near their computer device.
- Staff 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: ", £, $, %, ^, &, *, @, #, ?, !, €).
- Passwords or part of a password must not contain:
    - Any word(s) spelled backwards - (for example: drow, yadnom);
    - Any slang words - (for example: dubs, agro, bling);
    - Any word with numbers appended (for example: deer2000, password2012, Paul2468 etc);
    - Any words with simple obfuscation (for example: p@ssw0rd, l33th4x0r, @dm1n100, g0ldf1sh, etc);
    - Any names of fictional characters - (for example: frodo, shrek);
    - Any common keyboard sequences - (for example: qwerty);
    - Any personal information related to a user - (for example: user name, address, date of birth, school personnel number, car registration number, telephone number);
    - A sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);
    - The following sequence of letters - passwrd, passwd, pwrd, paswd, passwd.
- Staff who suspect their password is known by others must change their password immediately.
- Staff must ensure all default passwords which are supplied by a provider are changed in line with this policy as soon as could be reasonably expected.

21. Use of Email

- Teachers are encouraged to send email correspondence during normal working hours i.e. 0830 to 1700 Monday to Friday. Teachers may also consider scheduling emails to be sent during these times if they wish i.e. scheduling an email to be delivered at 0830 the following morning. Teachers are advised that they are under no obligation to respond to emails outside normal working hours.
- Teachers will use trusted school supplied email accounts for all communications.
- Teacher's use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Staff must not send any emails that are likely to cause distress or any material which is offensive, indecent, obscene, menacing, or in any way unlawful.
- The school network must not be used to send or distribute unsolicited commercial mail, commonly known as 'spam', in bulk or individually.
- Staff, as senders of emails, must not use false mail headers or alter the headers of mail messages in such a way as to conceal the identity of the sender.
- Where emails and attachments contain sensitive personal information, staff are required to password protect attachments to these emails. Attachments including sensitive personal information should be password protected i.e. ensuring only the recipient(s) with a password can open and access the contents of the email.
- Staff should not save copies of personal data to their own personal computers, phones, tablets, USB sticks, Hard Drives.

22. Use of the Management Information System, G-Suite & Microsoft 365

- The Management Information System, G-Suite & Microsoft 365 have been provided for teaching and learning.
- When using a personal (non-school supplied device) to access these ICT Resources the following applies:
    - Access is restricted to the browser i.e. staff are not permitted to download related apps. Accessing email (as an example) must be done through the browser only. Login details for these systems must not be saved / cached in the browser. In addition, staff are not permitted to download or store school related personal dtaa to their personal device.
    - Such devices must be secured by a password or a biometric access control (e.g., fingerprint scanner or facial recognition).
    - Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed.
    - Such devices must be configured so that they are automatically locked after being left idle for a set time e.g., 1 minute.
    - Such devices must not be used by family members or other persons. Passwords to such devices must be kept confidential and must not be shared with family members or third parties.
    - Care must be taken to avoid using such devices in a manner which could pose a risk to confidentiality, or personal data whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g., coffee shops or airports), or otherwise.
    - In the event that such a device is lost or stolen, or is suspected of having been lost or stolen, the Principal must be informed as soon as possible so that such steps as may be appropriate may be taken to mitigate the consequences of the loss.
    - Home Wi-Fi networks must be encrypted. Caution must be exercised when using public Wi-Fi networks as public Wi-Fi networks may not be secure.
    - If such a device needs to be repaired, appropriate steps must be taken to ensure that confidential information or personal data cannot be seen or copied by the repairer.
    - In the event that such a device needs to be disposed of, confidential material must be destroyed or wiped using a recognised method to put the data beyond recovery, to the satisfaction of Loreto College.
- In order to protect the information that is accessible on Management Information System, users must not divulge their logon details to third parties.
- Any concerns or queries must be forwarded and dealt by an Administrator with rights on the Management Information System, Microsoft 365 or G-Suite for Education.
- Staff must ensure they have strong passwords associated with their accounts i.e. a minimum of 8-12 characters with a mixture of upper case, lower case, number and symbols.
- 2 Factor Authentication will be used to verify staff logins.

23. Use of Social Media

Social Media Accounts

- Staff are not permitted to setup Social Media Accounts on behalf of / posing as Loreto College without the expressed written permission of the Principal.

Personal use of Social Media

- The Code of Professional Conduct published by the Teaching Council governs the use of Social Media sites by teaching staff.
- Non-teaching staff are expected to exercise sound judgement and maintain the highest professional standards while using social media in the school.
- All staff are encouraged to use the privacy settings on social media sites/apps and to keep updated on developments on privacy restrictions.

Unacceptable Uses of Social Media sites and the consequences of that Use

- All members of the school community are responsible for their own behaviour when communicating school related business using social media and will be held accountable for the school related content of their communications that they posted on social media locations.

Examples of Unacceptable Use of Social Media

- Posting of school content on personal social media accounts.
- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding, 'Liking' or commenting on school related material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the school's image or a person's reputation.
- Creating a fake profile that impersonates any other member of the school community.
- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchanging of inappropriate images or obscene material.
- Image based sexual abuse.

This list is not exhaustive.

While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of this policy. Disciplinary action will be taken in the case of inappropriate use of social media tools.

For teachers, infringements of this policy will be dealt with in accordance with the Teaching Council Code of Conduct and Disciplinary Procedures.

Please note that some inappropriate behaviour may be the subject of mandatory reporting to the relevant authorities or agencies.

24. Access to School Network

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

- Access rights and privileges to the school network domains and network resources will be allocated based on the specific requirement of each member of staff through the ICT Department.
- Accounts will be provisioned on a "least privileged access" basis i.e., a user is given the minimum levels of access or permissions needed to perform his/her function.
- Access to school network domains will be controlled by the use of individual user accounts.
- Where there is a need and with the approval of the Board of Management through the Principal, third party commercial service providers may request and be granted local access (on-site) and/or remote access to the school network domains and information management systems.
- Staff 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.

Only approved 3rd party contractors will be given access to areas housing school network servers and/or network and data communication equipment.

25. Information Storage

- Confidential or restricted personal data should be stored on a school network server (internal), school supplied trusted cloud or school supplied management information system (MIS) - Management Information System. Staff are not permitted to store school related personal data on a non-school supplied device.
- Confidential or restricted information stored on a school network server which is not stored as part of Management Information System must be held within a secure folder which is only accessible by authorised staff.
- School network servers are reserved for the hosting/storage of school business related systems, software applications and information only.
- Staff are not permitted to store non-school personal information (i.e. information which is of a personal nature and belongs to the user and not the school) on their school device.
- Staff are not permitted to store confidential or restricted personal data on a personal USB Stick, Hard Drive or Personal Cloud i.e. Personal Dropbox, Personal Google Drive, Box, personal iCloud etc.
- Under no circumstance should USB memory sticks (encrypted or otherwise) be used to transfer or store personal data, confidential information or restricted information – this will done using Sharepoint. Exceptions to this measure are limited to external authorised service providers working under the explicit instruction of the Senior Management Team.
- 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 as soon as is reasonably practicable.
- When the transfer is complete the photographic, video or audio recording on the recording device should be deleted.

Appropriate technical and organisational measures will be implemented to protect data stored on school devices and school servers. This will include Hard Drive Encryption and 2 Factor Authentication.

26. Information Disposal

Confidential and restricted information must be securely deleted when it is no longer required.

- All traces of confidential and restricted information must be purged from old school computers, smart devices, mobile computer devices, mobile phone devices and removable storage devices before they are reused within the school or recycled.
- The simple deletion or formatting of information stored on a device is not sufficient to remove all traces of the information. The information must be purged by either (1) using special sanitation software to overwrite the information a number of times, or (2) the hard disk must be degaussed (i.e. information is permanently purged using a powerful magnet) or (3) the physical destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc) on which the information is stored.
- Photocopiers and scanners which are fitted with hard disks must be purged of all confidential and personal data before they are disposed of or returned to the supplier.
- Computers and other ICT equipment which are leased from third parties must be purged of all confidential and personal data before being returned to the third-party leasing company.

Where the disposal of old school computer equipment and removable storage devices is outsourced to a commercial service provider the commercial service provider must:

- Ensure the operation of purging the computer equipment of all confidential and restricted information and the destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc) is carried out on-site before the equipment is taken off-site to a licenced WEEE recycling facility within Ireland.
- WEEE Recycling Facility to provide the school with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

27. Working from Home

School business is normally conducted in person within the school building. In exceptional circumstances, and at the discretion of the Board of Management, remote working / teaching / learning may be facilitated.

- Staff who are authorised by the Board of Management to work from home must take all reasonable measures to ensure that access to school ICT Resources including devices and software applications is kept secure and protected against unauthorised access, damage and / or loss.
- All work carried out by Staff on behalf of the school while working at home is done using approved software as per the "Approved ICT Resources List" held with the ICT Coordinator.
- No other platform which is their personal property, or the personal property of another household member should be used – the only exception to this is the ICT Department supporting persons using school domain accounts in the normal course of delivering services to the school.
- School devices must not be used by family members or other persons. Passwords to school devices must be kept confidential and must not be shared with family members or third parties.
- In the event that such a device is lost or stolen, or is suspected of having been lost or stolen, the Principal / ICT Department must be informed as soon as possible so that such steps as may be appropriate may to mitigate the consequences of the loss.
- All school supplied trusted software used by staff to work from home should be password protected in accordance with this policy.
- All confidential and restricted information which is accessed by them must be kept secure and confidential at all times.
- All school software and information provided to them are not accessed (including internet access) by members of their family, other household members or visitors.

28. 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.

29. Protocol for Live Meetings

Should the school need to revert to online meetings for both staff and student meetings.

- 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.
- Online Meetings where held i.e. Subject Department meetings, meetings with the Senior Management, Staff Meetings are permitted to take place on conferencing software as identified on the "Approved ICT Resources" list held with the ICT Coordinator.
- 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.
- Staff should consider all meetings on conferencing software as potentially sensitive and ensure that they are located in a quiet room where others cannot overhear the discussion.
- The use of WhatsApp is not permitted for communications involving personal data.
- Staff should exercise due care when live messaging / emailing during class i.e. ensure that the intended recipient(s) is being communicated with.
- The sharing of personal data should be limited to only those (i.e. staff) who need to know.
- Staff must take appropriate measures to secure data i.e. password protect any documents containing personal data and send this information only to those who need it via email.
- Minutes of meetings should be saved to the school's cloud and never locally to a personal storage device.

When teachers are conducting one to one session with students i.e. regarding Counselling, SEN, Disciplinary matters. The following protocol applies:

- School supplied conferencing software should be used to set up and conduct the meeting.
- Video may be used and, at either party's discretion may be turned off.
- The meeting shall not be recorded.
- If a student abruptly ends the meeting, the staff member is required to prepare a short report detailing the topic of discussion, matters raised etc. This report must be sent to the Principal and / or Deputy Principals within 24 hours of the meeting taking place.
- Where staff take notes, it is their responsibility to keep this data safe and secure.
- Where actions / next steps are agreed, they should be recorded and stored securely.

30. Periods of Absence

Staff should be conscious of ensuring school business can be maintained in their absence.

- During planned periods of absence (such as maternity / paternity leave, career breaks, holidays, when on training courses or working off-site for an extended period of time), staff should ensure wherever possible that the Principal or relevant colleagues have access to important school business related documents so that there is no delay in dealing with matters that are due to arise.
- Staff may adopt practices that ensures data / files can be easily accessed should the need arise i.e. Storing important data on a shared folder on the school cloud, copying appropriate persons on emails etc.

31. Staff Leaving the School

Staff should be conscious of their responsibilities when leaving Loreto College.

- Staff must return all school devices and accessories (where supplied), information (i.e. documents, files, important email messages etc) and other important items (e.g. master keys, classroom keys) to the Principal before they leave the employment of the school.
- The ICT Department will ensure that the management information system (Management Information System), G-Suite for Education, and network access accounts are revoked within 1 month of the staff member leaving the school.
- Staff leaving the employment of the school should also ensure they remove or delete all non-school personal information & email messages (i.e. information / email messages which are of a personal nature and belong to the user and not the school) from the devices used by them before they leave as it may not be possible to get a copy of this data once they have left the school.

32. Unacceptable Use

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

- Excessive personal use.
- Commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit.
- Political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions.
- To knowingly misrepresent the school.
- To transmit confidential or restricted information outside the school unless the activity has been authorised by the Principal.
- To store or transfer confidential or restricted information on a USB memory stick.
- To enter into contractual agreements inappropriately i.e. without authorisation.
- To create, view, download, host or transmit material (other than staff who are authorised by the school to access such material for research etc.) 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 waste the school's resources (e.g. staff time and ICT resources).
- 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.
- To install and use of software or hardware which could be used for the unauthorised monitoring of electronic communications within the school or elsewhere.
- To gain access to information management systems or information belonging to the school or others which you are not authorised to use.
- 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.

33. Acceptable Use Policy Acknowledgement

Print Name	Signed	Date