



01 271 8900



Loreto Avenue, Off Harbour
Road, Dalkey, Co. Dublin, A96
YC81.



office@LoretoAbbeyDalkey.ie

ACCEPTABLE USE POLICY

Effective Date: 27th January 2021

COVID-19/01/2020

APPROVED BY
Board of Management

DATE ISSUED
27th January 2021

ark.

We only work with schools

TABLE OF CONTENTS

Acceptable Use Policy.....	3
Responsibilities	4
Routine Monitoring	5
Confidentiality & Privacy	7
User Accounts & Passwords.....	8
Software & Electronic Media	9
ICT Devices & Equipment	10
Computer & Peripherals	10
The Child Trafficking And Pornography Act 1998.....	11
Access To School Network.....	13
Information Disposal	15
Working From Home	16
Protocol for Live Classes	17
Protocol for Live Meetings	18
Periods of Absence.....	19
Staff Leaving.....	19
Unacceptable Use	20
Student's Use Of Technology	21
Teacher's Use Of Technology	26
Appendix 1: Approved Technologies For Use.....	29

Acceptable Use Policy

Loreto Abbey Dalkey has invested significantly in the provision of technologies to aid productivity and facilitate remote teaching and learning (where needed) in the school.



Purpose

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

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

The purpose of this policy is to provide school staff and other 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.

This policy is mandatory and by accessing any ICT resources which are owned or leased by the school, users are agreeing to abide by the terms of this policy.

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 users (including school staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the school's ICT resources;
- All use (both personal & school business 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 any information stored on them remain the property of the school.
- Staff & students must ensure that they use ICT resources at all times in a manner which is lawful, ethical and efficient.
- Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.
- Staff 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 (Students) or Disciplinary Procedure (Staff). For breaches which do not warrant such action, those involved will be advised of the issue and given a reasonable opportunity to put it

Responsibilities

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

Roles & Responsibilities



- The Board of Management will approve the policy and ensure its development and evaluation.
- The Principal, Deputy Principal, ICT Postholder and Year Heads will be responsible for the dissemination of the policy including where relevant the application of sanctions.
- The ICT Postholder will schedule workshops and guest speakers to assist with the roll out of this policy as needed.
- The class teachers will outline to the various classes at an age-appropriate level unacceptable uses of ICT Resources to students.
- Class teachers and parents will advise children on safe internet use.
- Parents are expected to actively engage with their children, and to educate themselves on ICT issues including Social Media issues.
- Strategies to ensure online safety will be taught.
- Students will be permitted to use their managed device in school during class time. Specifically for the purpose of using approved technologies and associated apps directly in line with the class being taught at the time and only when directed by the teacher.
- Teachers will report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.
- The school community will provide support for students who have been victims of online bullying by implementing our *Anti-Bullying Policy*.



The school provides students with Internet access, access to desktop computers, virtual learning environments, online collaboration environments, online discussion forums, email and more.

As new technologies are developed that may prove valuable to our teaching and learning goals, Loreto Abbey Dalkey may provide access to them also. An approved list of technologies has been established and is available in the appendix.

Routine Monitoring

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

Routine Monitoring Purpose



- Helping to trace and resolve technical faults.
- Protecting and maintaining network and system security.
- Maintaining system performance and availability.
- Ensure 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.



While the school does not routinely monitor an individual user'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 Abbey Dalkey 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 child pornography must be reported to Gardai.

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

Personal Use

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

Exceptions



1. Is not excessive;
2. Does not take priority over their school work responsibilities;
3. It does not interfere with the performance and work of the user, other staff or the school;
4. Does not incur unwarranted expense or liability for the school;
5. Does not have a negative impact on the school in any way;
6. Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
7. 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.

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.

Policy



- Staff must respect the privacy and confidentiality of personal data at all times.
- Staff must not access personal data or information management systems unless they have a valid school related reason to do so or they have been granted permission by the Principal.
- 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 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 etc.
- 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 or 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.

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.

Policy



- Each authorised user will be assigned an individual account, a username and password which they may use to access a particular ICT resource. Only the individual to whom the account was assigned is permitted to use such account.
- 2 Step Verification will be enabled on accounts where service providers can facilitate this.
- Each user is responsible for all activities performed on any ICT device, information management system or software application while logged in under their individual account username and password.
- Staff / students must ensure all passwords assigned to them are kept secure. Staff / students must not write down their password(s) on or near their device.
- Staff / 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: ", £, \$, %, ^, &, *, @, #, ?, !, €).
- Passwords or part of a password must not contain:
 - A sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);
 - 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, car registration number, telephone number);
 - The following sequence of letters - passwrđ, passwd, pwrđ, paswd, passwd.
- Staff /students who suspect their password is known by others must change their password immediately.
- Staff must ensure all default passwords which are supplied by a vendor for new ICT devices and information management systems are changed at installation time.



Please refer to the school's Data Protection Policy which provides clear guidance regarding the accepted use of data in the school. This policy is available from the school website.

Software & Electronic Media

Each user 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.

Policy



- 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 devices where there is a valid school reason, and the software can add value to the users work 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 school.
- 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.



An Approved Software List (Back of this document) is maintained. Staff should refer to this list before downloading, accessing or using any 3rd party software in connection with school business.

ICT Devices & Equipment

All ICT devices and equipment are purchased through the agreed channels, national contract agreements or agreed ICT framework agreements.

Policy



- All ICT devices and equipment provided by the school remain the property of the school.
- Staff must not remove or borrow school ICT devices or equipment without the authorisation of the Principal.
- 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 Principal.
- Staff must not alter the hardware or software configuration of any school ICT device or equipment without the prior authorisation of the Principal.
- 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 must not use ICT devices and equipment (either in a school facility, while traveling or at home) if they have reason to believe it is dangerous to themselves or others.
- Staff must report all damaged, lost or stolen school ICT devices and equipment to ICT Coordinator.
- 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 school of any old ICT devices and equipment and they will facilitate the collection and disposal of the devices and equipment.
- 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.



ICT Equipment must be returned by staff before they leave the employment of the school. In addition, the school will then disable access to school software applications, networks etc.

Computer & Peripherals

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

Policy



- Staff should operate a clear screen policy when connected to the projector i.e. all applications displaying personal data should be closed.
- Staff must turn off their projector when leaving the class.
- Staff must disconnect from screen mirroring at the end of each class where relevant.
- 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.
- Confidential and restricted personal data, when printed, scanned or copied should where practical be collected from the printer, scanner or photocopier immediately.

The Child Trafficking And Pornography Act 1998

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

Policy



- The school has a duty of care to students under Safety, Health & Welfare at Work Act 2005 as well as the Child Trafficking And Pornography Act 1998.
- Every student in the school has a right to an effective learning environment in school at all times, free from risk of exploitation.
- 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.

Mobile Computer Devices & Smart Devices

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

Requirements



- School supplied devices will be provisioned accordingly i.e. for Apple devices, Apple School Manager will be deployed with staff using managed IDs.
- Staff must ensure that school laptops / mobile devices provided to them are protected at all times.
- Staff must take all reasonable steps to ensure that no damage is caused to the device and the device is protected against loss or theft.
- School devices will only be issued to staff who have signed acknowledgement of the Acceptable Use Policy (In appendix).
- All school devices must be registered with the ICT post holder so that they can be routed through the school network infrastructure and managed securely.
- School devices will be password protected in accordance with the user accounts and password policy on page 8.
- Passwords used to access school laptops, mobile computer devices and smart devices must not be written down on the device or stored with or near the device.
- All school supplied devices will be set up with a password / pin code / swipe gesture to gain access.
- When traveling by car, school laptops, mobile computer devices and smart devices should be stored securely out of sight when not in use. Staff are advised to avoid 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 school laptop, mobile computer devices or smart device in a public place 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 school laptops, mobile computer devices and smart 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).



Remote access connections to the school network, information management systems or school supplied cloud must be done so from a school laptop, mobile computer device or smart device.

Access To School Network

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

Policy



- 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.
- Access to school network domains will generally be controlled by the use of individual user account's.
- 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:
 - Disconnect any school ICT devices, equipment or removable storage devices to or from a school network domain without the prior authorisation of the Principal.
 - Connect any school ICT devices and equipment, laptop or smart device to an external network without the prior authorisation of the Principal.



All non-school staff given access to local server / comms rooms or other areas housing school network servers and/or network and data communication equipment must be accompanied by an authorized school staff member throughout their visit.

Information Storage

For security and legal reasons, the school's preferred position is that:

Policy



- All school confidential or restricted information is stored on a school network server (internal), school supplied cloud (Google Drive) or school supplied information management system (VS Ware).
- Confidential or restricted information stored on a school network server which is not stored as part of a school information management 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 must not store any 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 devices.
- Staff are not permitted to store confidential or restricted information i.e. personal data on a personal USB Stick, Hard Drive or Personal Cloud i.e. Dropbox, (non-school supplied) Google Drive, Box etc.
- Under no circumstance should USB memory sticks (encrypted or otherwise) be used to transfer or store school information management systems, data, confidential information or restricted information.
- Removable storage devices and school approved encrypted USB memory sticks except those used for backup purposes must not be used for the long-term storage of confidential or personal information.
- 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.
- When the transfer is complete the photographic, video or audio recording on the recording device should be deleted.



Appropriate technical and organizational measures will be implemented to protect data stored on school devices. This may include provisioning for Mobile Device Management, Hard Drive Encryption and 2 step verification.

Information Disposal

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

Policy



- 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) the information is stored on.
- 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.
- Provide the school with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

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.

Policy



- Staff who are authorised by the school 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, loss.
- All work carried out by Staff on behalf of the school while working at home is done so using the Core Technologies on the “Approved Technologies” List in Appendix 1.
- The storage of data is restricted to the school supplied devices and approved technologies listed in the the Appendix. No other platform which is their personal property, or the personal property of another household member should be used.
- All school supplied 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;
- All old printouts and other paper-based records that contain confidential or restricted information are shredded or disposed of securely and are not disposed along with their ordinary household rubbish;
- School Data on Personal Devices
 - When working from a personal device please ensure that you work from within the browser when working with personal data.
 - If you inadvertently download a document containing personal data, you must ensure that you delete the document from your hard drive.
 - Never save or cache the username / password on your personal device.
 - Once you are back at school, conduct a search of all devices to ensure that personal data is deleted / moved to the school cloud.

Protocol for Live Classes

Should the school need to revert to a remote teaching / learning approach in light of Covid-19.

Policy



- Each teacher and student will be assigned an individual account, username and password set which they can use to access a particular ICT resource.
- 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 behave as they would do in a normal classroom setting.
- Students are expected to conduct themselves with respect for both the teacher and their classmates.
- Escalation Policy – In the event of a student becoming disruptive in class the following escalation policy will be followed:
 - Student will be instructed to behave;
 - If the student does not comply, the student will be muted by the teacher to avoid further disruption;
 - If the disruption persists, the student's video will be turned off by the teacher;
 - Finally, if disruption persists the student will be removed from the online class and reported to the Year Head. At this point the school's code of behaviour will then apply.



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

- 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;

Protocol for Live Meetings

Should the school need to revert to online meetings for both staff and student meetings in light of Covid-19.

Policy



- Each teacher will be assigned an individual account, username and password which they can use to access a particular ICT resource.
- Online Meetings where held i.e. Subject Department meetings, meetings with the Principal / Deputy Principal, Staff Meetings are permitted to take place on conferencing software as identified on the Approved Technologies List.
- 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.
- 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 user's cloud and never locally to a personal storage device.



When teachers are conducting one to one sessions 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 Deputy Principal 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.

Periods of Absence

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

Policy



- 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 colleagues have access to important school business related documents and emails stored on their computer so that there is no delay in dealing with matters that are due to arise.
- Staff must backup and make sure relevant files/data/records are available for the covering/substitute teacher and/ or management and/or their subject department.
- Staff may adopt practices that ensures data / files can be easily accessed should the need arise i.e. Storing important data on a central folder on the school cloud, copying appropriate persons on emails, maintaining a filing system that is accessed by dedicated and approved keyholders etc.
- 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 on extended periods of absence such maternity leave, career break, carers leave.

Staff Leaving

Staff should be conscious of their responsibilities when leaving the school.

Policy



- Staff must return all school issued devices (iPads) 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 Principal must contact the ICT Postholder to ensure that the information management system and network access accounts belonging to staff leaving the employment of the school are revoked immediately once they leave the organization.
- 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 i.e. computer equipment before they leave as it may not be possible to get a copy of this data once they have left the school.

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.

Policy



- 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. unlicensed 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.
- 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.
- To gain access to information management systems or information belonging to the school or others which you are not authorized 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.

Student's Use Of Technology

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

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.
- Students will be provided with training in the area of Digital Literacy through formal timetabled classes.
- The use of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- Students will use Google Drive only (through their the school supplied G-Suite Account) for storage of digital files.
- 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.
- Cyber-bullying in any form is a very serious issue and will not be tolerated. Any student who experiences cyber-bullying must report it to the school. Any report of cyber-bullying will be taken seriously by the school and appropriate investigative procedures followed, in keeping with the school's Anti-Bullying Policy. Sanctions will be applied and guidance/counselling offered to students involved in cyber-bullying, in the interest of their well-being.

Internet Use



- Internet sessions will be supervised by a teacher, where possible. The school's Internet access is provided by PDST NCTE (School-Filtered Broadband). The school's Wi-Fi is available to all students and staff. The Wi-Fi is password protected for security reasons and to help ensure child and data safety.
- Non-school managed devices are not permitted to connect to the Wi-Fi without express permission from the Principal.
- 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 use the Internet for educational purposes only, not only as part of Computer Studies but in all Internet sessions on school grounds and as part of any school activity.

Internet Use (continued)



- 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.
- Downloading of materials or images by students, which is not relevant to their studies, is in direct breach of this Acceptable Use Policy.
- Students 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.
- 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 strictly forbidden for students to delete the work or files of other students from folders on the school network.
- It is strictly forbidden 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 on shared devices at the end of each Internet session e.g. Library. 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.

Email Use



- Students will use approved school e-mail accounts under supervision by, or permission from a teacher.
- Students will not send or receive 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.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving e-mail attachments is subject to permission from their teacher.
- Students will use their school email account for educational use, and will not use their personal email accounts to communicate with teachers.

Use of Social Media



- The purpose of having school social media accounts include:
 - Communication with the whole school community, especially parents / guardians, regarding specific school information, events & activities;
 - Foster parent / guardian involvement;
 - Communication with new or prospective parents / guardians;
 - Communication and engagement with the wider community regarding the positive advertisement and marketing of our school;
 - Communication and engagement with other schools and accounts with similar educational interests;
 - Monitor and regulate the school's online presence.
- Only official school social media accounts, or social media as instructed by a teacher, may be accessed by students on school grounds or as part of a school activity.
- Students' personal social media accounts may not be accessed during the school day or using the log-in details ascribed by the school.
- Users should not post anything on school social media channels that could be deemed as offensive – inappropriate or harmful comments/content will be removed immediately.
- Students will not attempt at any time to connect with any member of staff on that staff member's own personal social media account(s).
- Users should not ask to become "friends" with or "follow" staff as failure to respond may cause offence.

School Website / Social Media Accounts



- Photographs of students and in some cases including their name, may be published on our school website, app, on social media in line with the school's Data Protection Policy.
- The website/social media accounts will be regularly checked by the relevant co-ordinating teachers to ensure that there is no content that compromises the safety of students or staff.
- The publication of student work will be co-ordinated by a teacher.
- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focussing on group activities. Video clips may be password protected.
- Personal student information, including home address and contact details, will be omitted from school web pages.
- It is considered a serious breach of this policy for a student or member of staff to create and/or use a fake social media account in connection with school related business.

Recordings



- Only recordings permitted by a teacher in class are allowed. Students are forbidden from using any device to make an unauthorised recording of any sort in class, on a school outing or as part of a school activity.
- Students are forbidden from taking photos, video or sound recordings of anyone in the school (including students, staff, parents and visitors) unless permitted to do so by a teacher, and even then only with the consent of the individual(s) involved. Students must not share such material online without the clear permission of a teacher and only for educational or school promotional purposes.
- Students may be digitally recorded for educational purposes throughout their time in Loreto Abbey Dalkey. Such purposes include Classroom-Based Assessments, Leaving Certificate Vocational Programme, extra-curricular activities and participation in educational activities and outings.
- Recordings will be stored on school devices (e.g. digital cameras, school smart devices) and reasonable care will be taken to store recordings securely on the device and on the school's network. This includes both subject-related recordings and recordings of extra-curricular activities in which students are engaged.
- Some recordings will be brought to Subject Learning and Review Meetings by teachers in order to discuss and determine appropriate grade descriptors. Where it is necessary to store such recordings, reasonable care will be taken by teachers to ensure the safe-keeping of such recordings on the school server and / or school cloud.
- All recordings will take place in line with the Child Safeguarding Statement and Child Protection Procedures.
- Recordings will be deleted soon after a Subject Learning and Review Meeting.
- Recordings (e.g. photographs, short video clips) may also be used for promotional purposes of the school, e.g. via the school's official social media accounts.
- Consent is sought from parents regarding the use of photographs / video on an opt in basis.

Mobile Devices



- Students may use their school managed personal tablets or other devices as agreed with the Principal for educational purposes in specific classes using school approved technologies.
- Once such uses are finished, student devices must again be returned securely to their bags.
- It should be noted that it is a criminal offence to use a mobile device to menace, harass or offend another person (Section 10 of the non-fatal offences against the person Act 1997). Therefore, it may be necessary for the school to inform the Gardaí and/or Child Protection/Support Services in certain circumstances.
- Students using a mobile phone in school without a teacher's explicit permission, sending nuisance text messages, or the unauthorised taking of images with a Personal Device, still or moving, are in direct breach of this Acceptable Use Policy and the school's Code of Behaviour. Sanctions may be applied in such cases, as per the school's Code of Behaviour. Use of cameras on digital devices is only permitted with a teacher's permission.
- Where a phone is confiscated by a teacher it will be given to the Deputy Principal for safe-keeping and returned to the student, as per the Code of Behaviour.
- Students will be reminded of responsible device use and sanctions for misuse from time-to-time at Assemblies.
- In certain circumstances it may be necessary for a teacher/school management to inspect a student's device (e.g. where there are grounds to believe that the student has not complied with this policy). In such cases, two people will be present when the device is being inspected.
- Irresponsible or unethical use of mobile devices or school Internet will be considered a serious infringement of the Code of Behaviour and disciplinary action will be taken where this applies.
- It is imperative that students should always make contact with home through the school office during the school day in cases of illness, etc. A student should not use their mobile phone to send a text or make a phone call during the school day.
- Students are not allowed to charge their mobile phones in the school.

Examinations



- Mobile phones must be turned off and handed up to the examination supervisors while an examination is taking place. Mobile phones will be stored in a box at the top of the examination centre and students will not be permitted to access or use their mobile phone during examinations.
- Smart watches are not permitted during examinations.

Teacher's Use Of Technology

Various technologies are provided by the school and made available to staff to further their professional development and the education of the students in the school. Access to the school's supplied technologies is a privilege and not a right.

Any staff member or visitor who abuses this privilege will be immediately excluded from accessing and using these technologies.

Email Use



- Teachers are encouraged to send email correspondence during normal working hours i.e. 0900 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 0900 the following morning. Teachers are advised that they are under no obligation to respond to emails outside normal working hours.
- Teachers will use approved school 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 encrypt 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 will not save copies of personal data to their own personal computers, phones, tablets, USB sticks, Hard Drives;

Use of VS Ware



- In order to protect the information that is accessible on VS Ware, 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 VS Ware system.
- Where enabled, 2 Step Verification will be used to verify staff logins.

Use of Social Media



Use of Social Media

The use of WhatsApp is not permitted for communications involving personal data – iMessage on School iPads should be used as an alternative.

Personal use of Social Media

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

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 with social media and will be held accountable for the content of their communications that they post on social media locations.

Examples of Unacceptable Use of Social Media

- 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 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.

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 our Code of Behaviour. Disciplinary action will be taken in the case of inappropriate use of social media tools. This list is not exhaustive.

For teachers, infringements of this policy will be dealt with in accordance with the Code of Professional Conduct.

Use of Networks & Internet



- Staff must not use the school Internet for the transmission of illegal material. Staff shall refrain from sending or receiving any materials which may be deemed to be offensive, abusive, indecent, hard-core or paedophile pornography, defamatory, obscene, menacing or otherwise as prohibited by current and future statutes in force.
- Staff shall refrain from sending or receiving any material, which may be in breach of copyright (including intellectual property rights), confidence, privacy, or other rights.
- If you are in any doubt as the legality of what you are doing, or propose to do, you should either seek advice from the Principal or cease that usage.
- Student's work should never be shared on social networking sites or websites other than the school website. Sharing or making references to a student's work, especially if it could undermine the student, is not acceptable.
- Staff should be aware that the storage, distribution of, or transmission of illegal materials may lead to investigation and possible prosecution by the authorities.
- Staff may not gain or attempt to gain unauthorised access to any computer for any purpose.
- Staff must not send data via the internet using forged addresses or data which is deliberately designed to adversely affect remote machines (including but not limited to denial of service, ping storm, Trojans, worms, and viruses).
- Staff must not participate in the sending of unsolicited commercial or bulk email, commonly referred to as 'spam'.
- Staff are prohibited from running 'port scanning' or other software intended to probe, scan, test vulnerability of or access remote systems or networks except in circumstances where the remote user has given express permission for this to be done.
- Staff may not divulge their computer network passwords to third parties and must take all reasonable steps to ensure that such information remains confidential.
- Access to the computer network should only be made using the authorised logon name and password.
- The use of USB Sticks / Hard Drives for storage of personal data is prohibited.
- The use of the network to access and/or store inappropriate materials such as pornographic, racist, or offensive material is forbidden.
- In the interest of protecting the network from potential virus activity, the downloading of programs, games, screensavers, and wallpapers from the internet or uploading the same from disc or CD-ROM may only be carried out by the ICT Coordinator. This does not prevent Staff from using images taken and/or saved by them to set their desktop backgrounds.
- Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.
- Copyright of material must be respected, particularly with regard to the download and use of protected images for further use.

Appendix 1: Approved Technologies

Approved Technologies are technologies that the school has approved for use by relevant staff in their day to day work in the school. From time to time this list may be updated to reflect changes in how we do things or changing circumstances outside our control.

Core Software Applications (Teaching Staff)

- VS Ware;
- G-Suite for Education;
- Microsoft 365;
- iWork Suite;
- Apple School Manager;
- Zoom for Education;
- JAMF;
- Meraki;
- iDoceo;
- Online Learning Websites;

Core Software Applications (Administration)

- PPOD;
- ESI Net;
- Feemaster;
- Sage;
- Social Media Channels as determined from time to time;

Board of Management Approval



Board of Management of Loreto Abbey Dalkey, approved the revised Acceptable Use Policy on 27th January 2021.

Elis Humphreys

Signed: _____
Chairperson