Staff Acceptable Use, IT & Mobile Device Policy

Of

Jesus & Mary Secondary School,

Gortnor Abbey

School Patrons: Le Chéile Schools Trust clg.

Signed: _____
(Chairperson of Board of Management)

Signed: _____
(Principal)

Date: 8/6/26

Reviewed January 2025
Reviewed June 2026

Staff Acceptable Use, IT & Mobile Device Policy

Jesus & Mary Secondary School, Gortnor Abbey
Gortnor Abbey, Crossmolina, Co. Mayo.
T: 096 31194
E: office@gortnorabbey.ie

Issued By
The Ark HQ™

Date Issued
January 2025

Staff Acceptable Use, IT & Mobile Devices Policy

Document Title

Staff Acceptable Use, IT & Mobile Devices Policy

Revisions

No.	Status	Author(s)	Approved By	Office	Issue Date
Rev 01	Release	The Ark HQ™	Ark	Cork	January 2025

Circulation

Position	Office	Issue Date	Method
Senior Management	Jesus & Mary Secondary School, Gortnor Abbey	January 2025	Email
Board of Management	Jesus & Mary Secondary School, Gortnor Abbey	January 2025	Email
Staff	Jesus & Mary Secondary School, Gortnor Abbey	January 2025	Email

Table of Contents

1. Statement 4
2. Objectives 5
3. Responsibilities – Board of Management 5
4. Responsibilities – Senior Management 5
5. Responsibilities – ICT Department 6
6. Responsibilities – Administration Staff 6
7. Responsibilities – Teaching Staff 6
8. Routine Monitoring 7
9. Personal Use 8
10. Confidentiality & Privacy 9
11. User Accounts & Passwords 10
12. Software & Electronic Media 11
13. ICT Devices & Equipment 12
14. Computer & Peripherals 13
15. The Child Trafficking & Pornography Act 1998 13
16. Mobile Computer Devices & Smart Devices 14
17. Access to School Network 15
18. Information Storage 16
19. Information Disposal 17
20. Working from Home 18
21. Protocol for Remote Learning & Live Classes 19
22. Protocol for Live Meetings 20
23. Periods of Absence 21
24. Staff Leaving the School 21
25. Unacceptable Use 22
26. Staff Use of Technology 23
27. Appendix 1: Approved Technologies 27
28. Acceptable Use Policy Acknowledgement 28

Staff Acceptable Use, IT & Mobile Devices Policy

Jesus & Mary Secondary School, Gortnor Abbey 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. Jesus & Mary Secondary School, Gortnor Abbey (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 staff with clear guidance on the appropriate, safe and legal way in which they can make use of the school's ICT resources. By using any ICT resources which are owned or leased by the school, staff 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 teaching and non-teaching staff, contractors, sub-contractors, agency staff and authorised third party commercial service providers) of ICT resources.
- All use (both personal & school related) of the school's ICT resources.
- All connections to (locally/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 must ensure that they use ICT resources at all times in a manner which is lawful, ethical and efficient.
- Staff must respect the ICT devices and equipment provided for their use and take all reasonable steps to prevent damage, loss or misplacement.
- Staff 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 Disciplinary Procedure. 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.

Signed: _____
Chairperson Board of Management

Signed: _____
Principal

Date: _____

Date: _____

2. Objectives

- Protect and maintain the integrity of the facilities 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.

3. 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.
- Maintain an approved list of technologies.

4. Responsibilities – Senior Management

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

- Senior Management will be responsible for the dissemination of the policy including where relevant the application of sanctions.
- 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, 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 information technology.
- 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.

5. Responsibilities – ICT Department

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

- The ICT Department will be responsible for the technical implementation of the policy.
- To provide input on the implementation of the policy.
- To establish structures and procedures for the implementation of the Acceptable Use Policy.
- To make the necessary technical arrangements in order to demonstrate the AUP in practice.
- Where the AUP has been breached, report the breach to the Principal.
- To monitor the implementation of the policy.

6. Responsibilities – Administration Staff

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

- 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.

7. Responsibilities – Teaching Staff

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

- 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 computer and internet resources.
- To monitor the use of ICT resources.
- To record any violations of the Acceptable Use Policy and inform the Principal.
- To impose appropriate sanctions for violations of the Acceptable Use Policy.
- To report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.

8. Routine Monitoring

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

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

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.

Jesus & Mary Secondary School, Gortnor Abbey 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.

9. 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:

- Is not excessive.
- Does not take priority over their schoolwork responsibilities.
- It 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.

10. 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.

- Personal data must be processed exclusively on school-supplied devices authorised for such purposes, and staff must refrain from using personal devices for handling personal data, i.e. Handling personal data involves activities such as collecting, storing, accessing, updating, sharing, protecting, responding to requests, and maintaining records.
- 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 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 *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 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.

11. 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 Principal.

- 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.
- 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.

12. 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 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.

- 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 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.

13. ICT Devices & Equipment

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

- All ICT devices and equipment provided to staff remain the property of the school.
- 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.
- 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 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. In addition, the school will then disable access to school software applications, the MIS, networks etc. 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.

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 old and obsolete ICT devices and equipment and they will facilitate the collection and disposal of the devices and equipment.

14. 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 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.
- Confidential and restricted personal data, when printed, scanned or copied should where practical be collected from the printer, scanner or photocopier immediately.

15. The Child Trafficking & 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.

- 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.

16. Mobile Computer Devices & Smart Devices

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

- 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 that 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.
- All school devices must be registered with the ICT Department 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.
- 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 ICT 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 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 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 supplied device.

17. 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.
- 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:
    - 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 ICT.

Only approved 3rd party contractors will be given access to the local server / comms rooms or other areas housing school network servers and/or network and data communication equipment.

18. Information Storage

- Personal data must be processed exclusively on school-supplied devices authorised for such purposes, and staff must refrain from using personal devices for handling personal data, i.e. Handling personal data involves activities such as collecting, storing, accessing, updating, sharing, protecting, responding to requests, and maintaining records.
- Confidential or restricted personal data should be stored on a school network server (internal), school supplied cloud or school supplied management information system (the MIS).
- Confidential or restricted information stored on a school network server which is not stored as part of the MIS 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 school-related confidential or restricted personal data on a personal device, USB Stick, Hard Drive or Personal Cloud i.e. Personal Dropbox, Personal Google Drive, Box 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 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.
- The data subject rights will be respected where they object to the processing pursuant to Article 21(1) 'Right to Object' and there are no overriding legitimate grounds for the processing.

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

19. 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) 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.
- WEEE Recycling Facility to provide the school with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

20. 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 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 and / or 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 Appendix.
- No other platform which is their personal property, or the personal property of another household member should be used – the only exception here is contractors / self-employed persons using school domain accounts in the normal course of delivering services to the school.
- 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.

21. Protocol for Remote Learning & Live Classes

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

- Each teacher and student will be assigned an individual account, username and password 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 conduct themselves with respect for both the teacher and their classmates.

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.

22. Protocol for Live Meetings

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

- 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 Senior Management, 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 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, AEN, 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 Heads within 24 hours of the meeting taking place.
- Where staff take notes, it is there responsibility to keep this data safe and secure.
- Where actions / next steps are agreed, they should be recorded and stored securely.

23. 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 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 central folder on the school cloud, copying appropriate persons on emails, maintaining a filing system that is accessed by dedicated and approved keyholders etc.

24. Staff Leaving the School

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

- 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 (the MIS) and network access accounts belonging to staff leaving the employment of the school are revoked within 1 month once they leave 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 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.

25. 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.

- 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.
- 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.
- 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.

26. Staff 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

- Staff are encouraged to send email correspondence during the school day i.e., 0815 to 1800 Monday to Friday. Staff 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. Staff are advised that they are under no obligation to respond to emails outside their normal working hours.
- Staff will use approved school supplied email accounts for all communications.
- Staff'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 the MIS & Google Workspace

- In order to protect the information that is accessible on the MIS, 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 school the MISor Google Workspace.
- 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 Step Verification will be used to verify staff logins.

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 and ICT Department or cease that usage.
- Student's work should never be shared on social networking sites or websites other than the school website. Consent will need to be sought from the student before doing so. 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 Department. 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.

Use of Social Media

Personal use of Social Media

- The ***Guidance for Registered Teachers*** *About the Use of Social Media and Electronic Communication* published by the Teaching Council provides guidance on the use of Social Media by teaching staff – all staff are expected to review this document.
- Staff are advised to maintain a clear distinction between personal and professional profiles and interactions on social media.
- Use of digital platforms for communication with students should be conducted through official school channels or approved systems only.
- Regular review and appropriate adjustment of privacy settings on personal and professional social media accounts are recommended to safeguard personal information and professional integrity.
- Staff should be cautious about sharing content that could be misinterpreted or used inappropriately.
- Posts, comments, and interactions on social media should reflect the highest professional standards.
- Staff must avoid engaging in activities that could bring the profession or school into disrepute, including but not limited to, inappropriate discussions about students, parents, or colleagues.
- In the event of encountering or being the subject of inappropriate use of social media or electronic communication, staff should follow the school's protocol for reporting and addressing such incidents. This may include, but is not limited to seeking advice from school management, or contacting relevant authorities for serious matters.
- 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 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.

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

27. 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 –Staff

- Tyro;
- Google Workspace;
- Online Learning Websites;

Core Software – Management & Administration

- PPOD;
- ESI Net;
- Social Media Channels;

28. Acceptable Use Policy Acknowledgement

Print Name	Signed	Date