Communications Policy

1 Security and Communication

1.1 Personal Property

The Company does not accept responsibility (employee/faculty member/student's own risk) for any loss or damage to the property or personal belongings of any employee/faculty member/student which are brought onto or left on company premises or car parking areas.

1.2 Software

All software is the property of the company. The company strongly supports strict adherence to software vendors' licensing agreements. Any copying of software in a manner that is not consistent with the vendors' license agreement; participation (including during off-hours) in pirated software bulletin boards and similar activities are prohibited. It is forbidden to install any other programs without the written permission of the Company Director.

The company has virus protection software installed on all company hardware but there is still a high risk of viruses being received. All files via the Internet/disks/flash drives including e-mail attachments entering the company must be virus checked prior to their transfer for use to any company device. If you receive an external e-mail from an unknown source or a message which you feel is wrongly delivered, do not open it and contact the Company Director immediately. No exceptions are to be made to this policy, and any abuse of this policy will be subject to disciplinary action.

1.3 Data Protection Policy

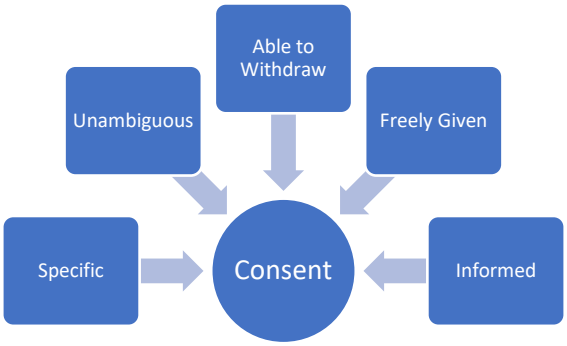
Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. Data Protection legislation (Data Protection Act 1988 and 2003 and the General Data Protection Regulation (GDPR). (the "Data Protection Acts") lay down strict rules about the way in which personal data and sensitive personal data are collected, accessed, used, and disclosed. The Data Protection Acts also permit individuals to access their personal data on request and confer on individuals the right to have their personal data amended, if found to be incorrect. This policy outlines Company policy to help ensure that we comply with the Data Protection Acts. Inquiries about this Data Protection Policy should be made to the Company Director. The Company is committed to adhering to the requirements of Data Protection legislation to ensure when handling an employee/faculty member/student's personal data that it is:

1. Processed lawfully, fairly and transparently.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Adequate and kept up to date where necessary.
5. Kept for no longer than is necessary where data subjects are identifiable.

6. Processed securely and protected against accidental loss, destruction or damage.

The Company will inform employee/faculty/students/contractors/guests of the purpose and use of their personal data and give a clear explanation of how it will be treated. Personal data is any information that identifies a data subject. Sensitive data is personal data that relates to a person's profile (e.g. race, health, criminal record, trade union membership, biometric data). At the time you join the Company, you are asked to give certain personal information for your records. Please remember to help us keep them up to date. Employee/faculty/students/contractors/guests(data subjects), will have the right to:

- **be informed** about the processing of their personal data.
- **rectification** if their personal data is inaccurate or incomplete.
- **access** to their personal data and supplementary information, and the right to confirmation that their personal data is being processed.
- **be forgotten** by having their personal data deleted or removed on request where there is no compelling reason for an organisation to continue to process it.
- **restrict** processing of their personal data, for example, if they consider that processing is unlawful, or the data is inaccurate.
- **data portability** of their personal data for their own purposes.
- **object** to the processing of their personal data for direct marketing, scientific or historical research or statistical purposes.



Consent

The Company is committed to review consent for existing employee/faculty/students/contractors/guests and to ensure all new employee/faculty member/students' consent is given at the time of information request. Employee/faculty/students/contractors/guests will be asked to give their consent independently or freely to the specific use, purpose or processing of that data where alternative lawful grounds for processing data are absent.

The Employment Cycle: The Company will request and maintain information during the employment life cycle.

Subject Access Request (SARs): The Company will provide an individual with a copy of the information they request without delay and within one month of request receipt. The Company will endeavour to provide employee/faculty/students/contractors/guests access to their information in

commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system. If complying with the request is complex or numerous, the deadline may be extended, and the individual will be informed within one month. The Company can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

The Company have an obligation to report actual or potential data protection compliance failures.

1.4 Email and Internet Code of Conduct

E-mail and the Internet are for business use only and private use is restricted on all devices. Every employee/faculty member/student has a responsibility to maintain the company's image, to use these electronic resources in a productive manner and to avoid placing the company at risk for legal liability based on their use. Employee/faculty/students/contractors/guests may not use Company electronic resources to create, host or transmit material which:

- is designed to cause annoyance, inconvenience, or needless anxiety to others.
- infringes the copyright of another person or organisation or infringe proprietary rights in any software.
- compromises the privacy of others or would destroy the integrity of computer-based information.
- contravenes current legislation or is in any way unlawful.
- Provides them with personal gain or profit.
- represents yourself as someone else
- interferes with job responsibilities (unreasonable/unwarranted time on the internet or on email activities).
- contains inappropriate, obscene, inflammatory, intimidatory, harassing, defamatory, disruptive or otherwise offensive language and anything that will reflect poorly on the name and professional reputation of the Company

The Company reserves the right to monitor all employee/faculty member/students' E-mails/Internet use on an ongoing basis. Accessing, downloading, or sending any indecent, obscene, pornographic, sexist, racist defamatory or other inappropriate materials, as well as the circulation of such materials is considered gross misconduct, and any breaches will be subject to disciplinary up to and including dismissal. This rule will be strictly enforced and is viewed as very serious with potential criminal liabilities arising therefrom. The Gardaí or other appropriate authority will be informed, where appropriate. Should you receive any offensive, unpleasant, harassing or intimidating messages you are requested to inform your manager or the IT Personnel immediately.

1.5 Social Media Policy

The Company recognise the importance of social media and know that social-media sharing is perfectly acceptable when directed by the Company that further enhances our business in a positive way. As with any communication, however, it is essential that we are responsible in our use of such media, especially regarding respecting employee/faculty member/students, customers, clients, the public and public disclosure of proprietary or sensitive information.

Think before you post: Keep in mind that most online social computing platforms are like public marketplaces; what's out there is available for all to see. On social platforms, the boundaries of professional and personal information are not always very clear. What you post may reflect on the Company, so if you are unsure whether certain content is appropriate to share online, don't post it.

Responsibility: You are personally responsible for your words and actions, no matter where you are, even in the online world. Please remember that when you participate in social media, you are speaking as an individual and not on behalf of the Company. Identify yourself using the first-person singular.

Employee/faculty/students/contractors/guests should be honest and respectful when using social media. When using social media in a personal or work capacity during or outside working hours, post on social media must not:

- Compromise the Company, disclose confidential data or disclose sensitive data.
- Damage the Company's reputation or brand.
- Breach copyright or data protection.
- Contain libel or defamatory content.
- Engage in bullying or harassment.
- Use of illegal, sexual or offensive content.
- Interfere with work commitments.
- Use the name of the Company to promote products or political opinions.

Social media content attributable to you which breaches the terms of this policy or the other related policies (Email and Internet Code of Conduct) is considered gross misconduct and may result in an investigation and disciplinary up to and including dismissal. Business contacts may not be added to personal social media accounts during the course of your employment.

1.6 CCTV Policy

A CCTV system is installed (both internally and externally) on the premises for the purpose of enhancing security of the building and its associated equipment. All employee/faculty/students/contractors/guests and visitors will be made aware that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance is intended for the purposes of:

- protecting the building and assets, both during and after hours.
- promoting the health and safety of employee/faculty/students/contractors/guests and visitors.
- preventing behaviour that might cause harm to employee/faculty/students/contractors/guests and visitors.
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism).
- verifying evidence as part of an investigation into misconduct and or gross misconduct.
- supporting the Gardaí in a bid to deter and detect crime.
- assisting in identifying, apprehending and prosecuting offenders.

Surveillance of employee/faculty/students/contractors/guests at work constitutes "data processing," and the Company complies with these principles as set out in the previous section. Any use of CCTV data will only be used in a disciplinary matter related to the intended purposes of use as stated above. The Company will ensure fair procedure in investigations using CCTV data before proceeding to disciplinary. The Company will ensure that notices are displayed around the workplace highlighting that CCTV is in operation.

1.7 Whistleblowing Policy

The Company is committed to the highest standards of openness, probity, and accountability and to achieve this enable employee/faculty/students/contractors/guests to voice concerns in a responsible and effective manner. A fundamental term of every contract of employment is that an

employee/faculty member/student will not disclose confidential information about the Company's affairs. Nevertheless, where an individual discovers information that they believe shows serious malpractice or wrongdoing within the Company, this information should be disclosed internally without fear of reprisal. This can be done independently of line management, but, in relatively minor instances, your team lead is the appropriate person to be told. This policy is intended to provide a support mechanism that describes how employee/faculty/students/contractors/guests are expected to behave should they find irregular activity happening in the Company. It is not designed to question financial or business decisions taken by the Company nor should it be used to reconsider any matters that have already been addressed under harassment, complaint, disciplinary or other procedures. It is reasonable to expect all employee/faculty/students/contractors/guests to use this procedure, rather than air complaints outside the Company. The value of a whistleblowing policy is to:

- demonstrate that all employee/faculty/students/contractors/guests are accountable for behaving in a responsible and honest manner.
- make it clear that everyone is responsible for reporting a lack of probity.
- show that concerns within the Company can be reported internally without fear of reprisal.
- outline the steps an employee/faculty member/student should take should they find any wrongdoing.
- reinforce the need for confidentiality in relation to information about the employer's affairs.
- criminal activity.
- improper conduct or unethical behaviour.
- attempts to conceal any of these.

Confidentiality: The Company will treat all such disclosures in a confidential and sensitive manner. The identity of the individual making the allegation may be kept confidential as long as it does not hinder or frustrate any investigation. The investigation process may reveal the source of the information, however and the individual making the disclosure may need to provide a statement as part of the evidence required.

Anonymous allegations: This policy encourages individuals to put their name to any disclosures they make. Concerns expressed anonymously are much less credible, but they may be considered at the discretion of the Company and the factors to be considered will include (a) the seriousness of the issues raised (b) the credibility of the concern and (c) the likelihood of confirming the allegation from attributable sources.

Untrue allegations: If an individual makes an allegation in good faith that is not confirmed by subsequent investigation, no action will be taken against that individual. In making a disclosure the individual should exercise due care to ensure the accuracy of the information. If, however, it is malicious or vexatious and particularly if he or she persists in making them disciplinary may be taken against that individual. In an extreme case, malicious or wild allegations could give rise to legal action on the part of the persons complained about.

Protection: This policy is designed to offer protection to those employee/faculty/students/contractors/guests who disclose such concerns, provided the disclosure is made in good faith and in the reasonable belief of the individual making the disclosure There is no protection from internal disciplinary procedures to those who choose not to use the procedure.

Procedures for making a disclosure: The employee/faculty member/student who receives and takes note of the complaint must pass this information to the appropriate designated investigating officer as soon as is reasonably possible.

- Complaints of malpractice will be investigated by the Company Director unless the complaint is against that individual or is in any way related to the actions of that incumbent.

- Complaints against the Company Director should be passed to another Director, who will nominate an appropriate investigating officer.

The complainant has the right to bypass the line management structure and take their complaint direct to the Company Director who has the right to refer the complaint back to the manager, if he or she feels that the manager can investigate the complaint more appropriately, without any conflict of interest. Should none of the above routes be suitable or acceptable to the complainant, the complainant may approach one of the individuals who has been designated as an independent point of contact under this procedure. They can advise the complainant on the implications of the legislation and the possible internal and external avenues of complaint open to them. If there is evidence of criminal activity, the investigating officer should inform the Garda Síochána. The Company will ensure that any internal investigation does not hinder a formal Garda Síochána investigation.

Timescales: Due to the varied nature of these sorts of complaints which may involve internal investigators and/or the Garda Síochána, it is not possible to lay down precise timescales for such investigations. The investigating officer will ensure that the investigations are undertaken as quickly as possible without affecting the quality and depth of those investigations. The investigating officer will send a written acknowledgement of the concern to the complainant as soon as practically possible and report back to them in writing thereafter outlining the outcome of the investigation and the action proposed. If the investigation is a prolonged one the investigating officer should keep the complainant informed, in writing of progress and of the likely timeframe for conclusion. All responses to the complainant will be in writing and sent to their home address.

Investigation: The investigation officer should follow these steps:

- Full details and clarifications of the complaint should be obtained.
- The investigating officer should inform the employee/faculty member/student against whom the complaint is made as soon as is practically possible. The employee/faculty member/student will be informed of their right to be accompanied (a colleague of the employee/faculty member/student's choice) at any future interview or hearing held under the provision of these procedures.
- The investigating officer should consider the involvement of the Company's auditors and the Garda Síochána at this stage and should consult with the Company Director .
- The allegations should be fully investigated by the investigating officer with the assistance of other individuals or bodies, where appropriate.
- A judgment concerning the complaint and validity of the complaint will be made by the investigating officer. This judgment will be detailed in a written report containing the findings of the investigations and reasons for the judgment. The report will be passed to the Company Director as appropriate.
- The Company Director will decide what action to take. If the complaint is shown to be justified, they will invoke the disciplinary or other appropriate procedures.
- The complainant should be kept informed of the progress of the investigations and, if appropriate, of the final outcome.
- If appropriate, a copy of the outcomes will be passed to the Company's auditors to enable a review of the procedures.
- If the complainant is not satisfied that their concern is being properly dealt with by the investigating officer, they have the right to raise it in confidence with one of the designated persons described above.

If the investigation finds the allegations are unsubstantiated and all internal procedures have been exhausted, but the complainant is not satisfied with the outcome of the investigation, the Company recognises the lawful rights of employee/faculty/students/contractors/guests and ex-

employee/faculty/students/contractors/guests to make disclosures to prescribed persons (such as the Health and Safety Authority inspectors) or where justified, elsewhere.

1.8 Monitoring & Compliance

Employee/faculty/students/contractors/guests should never consider electronic communications to be either private or secure. The company has the right to record and monitor the activities of all users on company systems and devices. It is our objective that such monitoring will not be required on an on-going basis and will be used to review usage and audit practices. However, the company retains to right to monitor (intercept and read) each individual's e-mail, online use, mobile devices, network, and PC activity to ensure the protection of all employee/faculty/students/contractors/guests and that there is no abuse of privilege. No employee/faculty member/student should have an expectation of privacy in relation to electronic records or communications. Notwithstanding the company's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employee/faculty/students/contractors/guest sand accessed only by the intended recipient. Employee/faculty/students/contractors/guests are not authorised to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior approval from the Company Director . However, the confidentiality of any message should not be assumed.

Any employee/faculty member/student found to be abusing the company electronic communication system or not operating in line with policies and procedures outlined in this section will be subject to disciplinary up to and including dismissal. This includes any attempt to circumvent system security, including firewalls put in place to protect the company, inappropriate use of e-mail, Internet and other electronic communications services.

Version	Date	Details	Author(s)	Approved by	Approval Date
1	Jan 2019	Initial creation	T.Mulhearne	A.Laste	
2	Nov 2023	Update & Review	T.MulHearne/A.Laste	P.Glynn	
3	Jul 2025	Policy updates to incorporate Faculty & students as well as staff as per PHECC QRF review.	T.Mulhearne/A.Laste	P.Glynn	
4	Aug 2025	Inclusion of approval date.	A.Laste	P.Glynn	25/08/2025