The Irish Nurses & Midwives Organisation
The Whitworth Building
North Brunswick St
Dublin 7

Data Protection Policy

Contents

Version History:

Version:	Date:	Specific Updates:
1.0	27th May 2018	Policy Distribution
2.0	30th May 2019	Policy Review – minor technical updates.
3.0	3rd August 2020	Policy Review – Addition of Appendix R re internal processing of data access request, and minor technical updates.
3.1	31st August 2020	Minor review, clerical error in previous version. Also, inclusion of information re Covid-19 Declaration Form
4.0	23rd February 2023	Substantive Review Inclusion of card payment processing.
5.0	28th September 2023	Minor clerical update.
6.0	15th March 2024	Information added re transfer of data to the United Kingdom, and updated data privacy notice for members.
7.0	11th June 2024	Appendix U re Use of instant messaging platforms

1. Introduction

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The Irish Nurses and Midwives Organisation ("the Organisation") needs to collect and use personal data about its partners, staff and other individuals who come into contact with the Organisation. Those individuals ("data subjects") have privacy rights in relation to the processing of their personal data. Additionally, members of the Organisation engage with us in relation to a wide range of issues, of often a sensitive nature, relating to their employment and they do so on the basis of the confidential nature of the service we provide. Therefore, they have a reasonable expectation of privacy and confidentially when engaging with the Organisation in matters relating to their employment and the data associated with such engagement. The Organisation must therefore comply with the EU General Data Protection Regulation ("GDPR") and the Irish Data Protection Acts, 1988 to 2018 (the "DPA") – known collectively in this policy as "the Data Protection Acts". The Data Protection Acts confer rights on individuals as well as responsibilities on those who process personal data.

2. Personal Data and 'Special Categories' of Personal Data

'Personal data' means any information relating to an identified or identifiable living person ('data subject'). It is important to note that the definition of personal data now specifically includes information such as identification numbers, location data and online identifiers. In practice, any data about a living person who can be identified from the data available (or potentially available) will count as personal data. This will include reversibly anonymised ('pseudonymised') data i.e. replacing any identifying characteristics of data with a value which does not allow the data subject to be directly identified (pseudonym). Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data. Examples of personal data can be found in Appendix F.

Stronger safeguards and requirements are required for 'special categories of data' (previously known as 'sensitive personal data') under the GDPR. This refers to data falling under the following categories:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union partnership
- Data concerning health
- Data concerning a person's sex life or sexual orientation
- Genetic data
- Biometric data.

Personal data falling under these categories can be processed only under specific circumstances, which are described in Article 9(2) of the GDPR (See Appendix B).

Personal data relating to criminal convictions and offences, while not included in the list of 'special categories' of personal data, have extra safeguards applied to processing them (see Appendix C).

Please see the Definitions section of this Policy for details on the terms used in this policy.

3. Purpose

This policy is a statement of the Organisation's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts. It sets out responsibilities for all managers, employees, contractors and anyone else who can access or use personal data in their work for the Organisation.

4. Scope

4.1 What information is included in this Policy?

This policy applies to all personal data created or received in the course of Organisation's business in all formats, of any age. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone.

4.2 To whom does this Policy apply?

This policy applies to:

- any person who is employed or engaged by the Organisation who processes personal data in the course of their employment or engagement;
- any member of the Executive Council of the Organisation who processes personal data in the course of their duties;
- any member of the Executive Council of the Organisation who processes personal data in the course of their duties;
- any local representative, in the meaning of our Rule Book, of the Organisation who processes personal data in the course of their studies;
- individuals who are not directly employed by the INMO, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the INMO.

Hereinafter these are collectively referred to as "partners".

4.3 Where does the Policy apply?

This policy applies to all locations from which personal data held by the Organisation is accessed, including home use.

5.Data Protection Policy

The Organisation undertakes to perform its responsibilities under the legislation in accordance with the Data Protection Acts.

5.1 Data Protection Principles

The Organisation is responsible for, and must be able to demonstrate, compliance ("accountability") with the following Data Protection Principles:

Personal data shall be:

- Processed lawfully, fairly and in a way that is transparent to the data subject ("lawfulness, fairness and transparency");
- Collected, created or processed only for one or more specified, explicit and lawful purpose ("purpose limitation");
- Adequate, relevant and limited to what is necessary for those purposes ("data minimisation");
- Kept accurate and, where necessary, up-to-date ("accuracy");
- Retained no longer than is necessary ("storage limitation");
- Kept safe and secure ("integrity and confidentiality")
- These provisions are binding on every data controller, including the INMO. Any failure to observe them would be a breach of the Data Protection Acts. Further explanation of each principle is outlined below.

1. Process personal data lawfully, fairly and transparently

When the Organisation collects personal data, it has to make certain information available to the person the data relates to. This applies whether the information is collected directly from the individual or from another source. This information must be provided via a Data Protection Notice (or Privacy Statement in the case of a website). In addition, the Organisation must have a legal basis for processing the data. These legal bases are specifically defined in the Data Protection Acts and are set out below.

<u>Data Protection Notices</u>

When is a Data Protection Notice required?

- Where information is being collected directly from an individual, a Data Protection Notice must be provided at the point at which the data is collected.
- Where information is obtained from another source, a Data Protection Notice must be provided:
    - at least one month after obtaining the data;
    - if personal data is to be used to communicate with the data subject at the latest at the time of the first communication with the data subjects;
- if disclosure to another recipient is envisaged, at the latest when personal data are first disclosed.

<u>What needs to be included in a Data Protection Notice?</u>

Data Protection Notices must contain specific information (set out in the legislation) which informs data subjects of:

- who is collecting the data;

- why it is being collected;
- what legal basis is being relied upon to process the data;
- how it will be processed;
- how long it will be kept for;
- who it will be disclosed to.

What rights people have in relation to their own data (see section 5.6 – Data Subject Rights below).

Individuals must also be made aware of:

- the right to lodge a complaint with the Data Protection Commission
- the lawful basis for the processing and the consequences of failure to provide the data
- the existence of automated decision making, including profiling.

Legal Basis for Processing

In order to collect and process personal data "lawfully", the Organisation must have a legal basis for doing so. There are six available legal bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and the relationship with the individual. The six legal bases, set out in Article 6(1) of the GDPR, are as follows:

- Consent: the individual has given clear consent for the Organisation to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract the Organisation has with the individual, or because they have asked the Organisation to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for the Organisation to comply with the law.
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for the Organisation to perform a task in the public interest or for its official functions.
- Legitimate interests: the processing is necessary for the legitimate interests of the Organisation or a third party.

The Organisation must determine its legal basis before beginning to process personal data, and should document it in its Data Protection Notices and in the Organisation Register of Personal Data.

In cases where the Organisation relies on consent as a condition for processing personal data, it must:

- Obtain the data subject's specific, informed and freely given consent
- Ensure that the data subject gives consent by a statement or a clear affirmative action
- Document that statement/affirmative action
- Allow data subjects to withdraw their consent at any time without detriment to their interests.
- Further information on consent is documented in Appendix D.

In the case of personal data relating to special categories of data, it is necessary for the processing to be covered both by a legal basis and by a special category condition set out in Article 9 of the GDPR (see Appendix B). In the case of personal data relating to criminal convictions and offences, it is necessary for the processing to be covered both by a legal basis and by a separate condition for processing this data in compliance with Article 10 of the GDPR (see Appendix C). Both of these types of processing need to be documented to demonstrate accountability and compliance.

See Appendix A for further details of lawful bases.

2: Process personal data only for one or more specified, explicit and LAWFUL purposes ("purpose limitation")

Partners must:

- only keep personal data for purposes that are specific, lawful and clearly stated (in the data protection notice);
- only process personal data in a manner which is compatible with these purposes;
- treat people fairly by using their personal data for purposes and in a way they would reasonably expect;
- ensure that the data is not reused for a different purpose that the individual did not agree to or would reasonably expect.
- ensure that the collection and processing of the data is lawful by meeting one or more of the lawful bases (See Appendix A).

3: Ensure that personal data being processed is adequate, relevant and not excessive ("data minimisation")

Partners should only collect the minimum amount of personal data from individuals that is needed for the purpose(s) for which it is kept (and referred to in the data protection notice).

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept. Special attention should be paid to the protection of special categories of personal data, the disclosure of which would normally require explicit consent or one of the other specified lawful bases (see Appendix A).

4: Keep personal data accurate and, where necessary, up-to-date ("accuracy")

Partners must ensure that the personal data being processed is accurate and, where necessary, kept up-to-date. Partners must ensure that local procedures are in place to ensure high levels of personal data accuracy, including periodic review and audit.

5: Retain personal data no longer than is necessary for the specified purpose or purposes ("storage limitation")

Partners must be clear about the length of time for which personal data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal data, then that data should be routinely deleted.

Partners must comply with the Organisation's Records Management Policy, and apply the Organisation's Records Retention Schedules to keep records and information containing personal data only so long as required for the purposes for which they were collected.

The legislation allows for data to be stored for longer periods kept insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals.

6: Keep personal data safe and secure ("integrity and confidentiality")

Partners must take appropriate security measures to protect personal data from:

- unauthorised access
- inappropriate access controls allowing unauthorised use of information
- being altered, deleted or destroyed without authorisation by the "data owner"
- disclosure to unauthorised individuals
- attempts to gain unauthorised access to computer systems e.g. hacking
- viruses or other security attacks
- loss or theft
- unlawful forms of processing.

While the Data Protection Acts do not specify the necessary security measures to be taken, they require that the state of technological developments, the nature of the data and the degree of harm that might result from unauthorised or unlawful processing should be taken into consideration.

The Organisation has its own policies on security, the principles of which are addressed in the Record Management and IT policies, which must be adhered to at all times.

Where transferring personal data to another country outside the European Union, appropriate agreements and auditable security controls to maintain privacy rights must be put in place. It is not envisaged that the Organisation will engage in this activity, however, should this become necessary the appropriate controls will be adopted. See section 5.11 below.

Advice and guidance must be sought from the Organisation's Senior Management Team and Data Protection Officer where you are considering a transfer of data outside of the EEA.

<u>Accountability</u>

The GDPR states that the data controller shall be responsible for, and be able to demonstrate compliance with the above principles ("accountability"). This means that we must:

- maintain relevant documentation on all data processing activities (see 5.2 below);
- implement appropriate technical and organisational measures that ensure and demonstrate that we comply;
- implement measures that meet the principles of privacy by design and by default (see 5.3 below), such as:
    - data minimisation;

    - pseudonymisation;
    - transparency; and
    - creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.
- record all data security breaches (see 5.5 below).

5.2 Records of Processing Activities: Registers of Personal Data

In order to maintain documentation on processing activities, the Organisation has created a central Register of Personal Data which documents what personal data we hold as a Data Controller, what we use it for, the legal basis we are relying on in order to process the data, who we may share it with, where it is held and how long we keep it.

Every department/unit/office in the Organisation is required to record the information required to compile the Registers. This process is coordinated by the Data Protection Officer.

5.3 Privacy by Design and by Default

Privacy by design and by default is written into Article 25 of the GDPR.

Privacy by Design states that any action an organisation undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the Organisation must ensure that privacy is built in to a system during the whole life cycle of the system or process.

Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. If more information than necessary to provide the service is disclosed, then "privacy by default" has been breached.

Partners must apply the principles of Privacy by Design and by Default when processing any personal data by:

- Performing a Data Protection Impact Assessment (DPIA) – see section below – where data processing is likely to result in a high risk to the rights and freedoms of individuals, especially when a new data processing technology is being introduced.
- Performing a DPIA where systematic and extensive evaluation of individuals is to be carried out based on automated processing (profiling), large scale processing of special categories of data and personal data relating to criminal convictions.
- Collecting, disclosing and retaining the minimum personal data for the minimum time necessary for the purpose;
- Anonymising personal data wherever necessary and appropriate.

5.4 Data Protection Impact Assessments (DPIA)

When the INMO processes personal data, the individual whose data we are processing is exposed to risks. A Data Protection Impact Assessment (DPIA) is the process of systematically identifying and minimising those risks as far and as early as possible. It allows the INMO to identify potential privacy issues before they arise, and come up with a way to mitigate them.

The INMO will conduct a DPIA in any instance where our activities are likely to result in a high risk to the rights and freedoms of individuals, especially when a new data processing technology is being introduced.

5.5 Personal Data Security Breaches

The Organisation will take all necessary steps to reduce the impact of incidents involving personal data by following the Organisation's Personal Data Security Breach Management Procedure. Where a data breach is likely to result in a risk to the rights and freedoms of data subject, the Data Protection Officer will liaise with the Data Protection Commissioner's Office and report the breach within 72 hours of discovery. The Data Protection Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

Partners who discover a personal data security breach must immediately inform their Head of Department/Unit who will contact the Data Protection Officer following the above procedure. It is important that all Partners act quickly and report any suspected incident without delay.

5.6 Data Subject Rights

The GDPR provides the following rights for individuals:

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. See section above on Data Protection Notices.

The right of access

Data subjects are entitled to make an access request under the Data Protection Acts for a copy of their personal data and for information relating to that data. This must be complied with within one calendar month.

If a data access request is received by the Organisation, the recipient should forward it immediately to the Organisation's Data Protection Officer (contact details below) who will respond to the request on behalf of the Organisation, consulting with staff in relevant offices/departments and taking into account the narrow exemptions set out in the legislation.

Please refer to the INMO's Data Access Request Procedure.

In certain circumstances, the Organisation is able to avail of exemptions from the restrictions in the Data Protection Acts (e.g. disclosure required by law). These exemptions are subject to

strict conditions, and should only be availed of where authorised by the Organisation's Data Protection Officer.

The personal information of a data subject must not be disclosed to a third party, be they parent/relative, potential employer, employer, professional body, etc. without the consent of the individual concerned.

The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The Organisation must respond to a request within one calendar month. In certain circumstances, the Organisation can refuse a request for rectification.

All requests for rectification of personal data should be notified to the Data Protection Officer without delay who will advise further on the steps to be taken to respond to the request.

The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The Organisation must respond to a request within one calendar month. The right to erasure is not absolute and only applies in certain circumstances.
All requests for erasure of personal data should be notified to the Data Protection Officer without delay who will advise further on the steps to be taken to respond to the request.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, the Organisation is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing and the Organisation must respond within one calendar month.

All requests to restrict the processing of personal data should be notified to the Data Protection Officer without delay who will advise further on the steps to be taken to respond to the request.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

All requests in relation to portability of personal data should be notified to the Data Protection Officer.

The right to object

Individuals have the right to object to:
1. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling):

- Individuals must have an objection on "grounds relating to his or her particular situation".
- You must stop processing the personal data unless:
    - you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
    - the processing is for the establishment, exercise or defence of legal claims.
- You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.
- This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

2. direct marketing (including profiling)

- You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- You must deal with an objection to processing for direct marketing at any time and free of charge.
- You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.
- This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".
- Data subjects must be given the option to opt out of further communications each and every time they are contacted. They must also be given the opportunity to segment their preferences.

3. processing for purposes of scientific/historical research and statistics.

- Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes. If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

Rights in relation to automated decision making and profiling

- You must offer a way for individuals to object online, however, this is not an activity undertaken by the Organisation.

5.7 External Data Processors

It is occasionally necessary for the Organisation to engage the services of external suppliers. If the service involves the external hosting of personal data (such as staff and member data) by the supplier on behalf of the Organisation, a number of steps must be taken before any personal data can be disclosed to the supplier:

- the Data Protection Officer must conduct a DPIA;
- the results of that assessment will be considered by the Senior Management Team;
- a decision to proceed will only be taken by the General secretary, or her designate, when all necessary contractual, security and other controls are assured.

5.8 Transfers of Personal Data Outside of the E.U.

It is not generally the practice of the INMO to transfer personal data outside of the E.U., however, it may be the case that personal data may be transferred to the United Kingdom flowing from the management of our CRM IT infrastructure.

Where this does occur the GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

- You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.
- Adequate safeguards may be provided for by:
    - a legally binding agreement between public authorities or bodies;
    - binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
    - standard data protection clauses in the form of template transfer clauses adopted by the Commission;
    - standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
    - compliance with an approved code of conduct approved by a supervisory authority;
    - certification under an approved certification mechanism as provided for in the GDPR;
    - contractual clauses agreed authorised by the competent supervisory authority; or
    - provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

In the context of the CRM used by the INMO, the development and management of IT infrastructure related to that system is currently contracted to a company in the United Kingdom. This means that data may be transferred to the UK in that context.

Noting the requirements of the GDPR – on 28th June 2021 the EU Commission issued an adequacy decision under the GDPR which means that personal data can now flow freely from the European Union to the United Kingdom where it benefits from an essentially equivalent level of protection to that guaranteed under EU law. This decision has a sunset clause which means it will expire in 2025, this matter will be kept under review by the INMO.

In addition, the INMO has a data transfer agreement with our contractor which protects the rights of data subjects.

If there is a future intention to transfer personal data outside of the E.U. in other contexts the Data Protection Officer, in the first instance, will seek the appropriate legal advice and will advise the Senior Management Team. A decision on such an activity will be taken by the General Secretary or her Designate.

5.9 Marketing / Mailing Lists / Electronic Privacy Regulations

The Electronic Privacy Regulations 2011 (SI 336 of 2011) sit alongside the Data Protection Acts. They give people specific privacy rights in relation to electronic communications and contain specific rules on:

- Marketing calls, emails, texts and faxes
- Cookies (and similar technologies)
- Keeping communications services secure; and
- Customer privacy regarding traffic and location data, itemised billing, line identification, and directory listings.

While primarily aimed at electronic communications companies (telecommunications companies and internet services providers), the Regulations also apply to any entity (such as the INMO) using such communications and electronic communications networks to communicate with Partners, e.g. by telephone, via a website or over email, etc.

Unsolicited direct marketing is one of the main sources of complaint from individuals to the Data Protection Commissioner and anyone who fails to comply with the E-Privacy Regulations can be prosecuted as each unlawful marketing message or call constitutes a separate offence.

It is imperative that the necessary marketing opt-ins and opt-outs (via a data protection notice or otherwise) are in place before using personal data for marketing purposes. The Data Protection Commissioner's office provides further guidance on this matter. The INMO provides an opt in provision in our membership application process in relation to marketing communications. Our Data Protection Notice to Members also provides information on opting out at any time.

Where Partners process personal data to keep people informed about Organisation activities and events they must provide in each communication a simple way of opting out of further communications.

5.10 Personal Data relating to Criminal Convictions/Offences (incl. Garda Vetting)

To process personal data about criminal convictions or offences, the Organisation must have both a lawful basis under Article 6 of the GDPR and either legal authority or official authority for the processing under Article 10. This must be established before processing begins and must be documented. See Appendix C for further information.

5.11 Profiling and/or Automated Decision Making

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work or studies, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

While the law recognises profiling and automated decision-making can be useful for individuals and organisations, GDPR restricts profiling and gives data subject rights around profiling-based decisions. For example, there is a general prohibition on 'solely' automated processing producing 'legal' or 'similarly significant' effects unless permitted by law and the transparency requirements (set out in section 1 above) are complied with.

There is a distinction between the concepts of profiling and automated decision-making. There are three ways in which profiling can be used in practice:

- general 'profiling', defined in Article 4(4) GDPR
- human decision-making based on profiling; and
- purely automated decision-making under Article 22 GDPR, which includes profiling legal effects concerning, or similarly significantly affecting, the data subject.

Advice and guidance on profiling can be sought from the Organisation's Data Protection Officer, however, profiling and automated decision making are not a feature of the activities of the INMO.

5.12 CCTV

All usage of CCTV other than in a purely domestic context must be undertaken in compliance with the requirements of the Data Protection Acts. Extensive guidance on this issue is available on the Data Protection Commissioner's website.

In summary, all uses of CCTV must be proportionate and for a specific purpose. As CCTV infringes the privacy of the persons captured in the images, there must be a genuine reason for installing such a system.

The INMO has closed circuit television cameras ("CCTV") located in its various offices covering buildings, some internal spaces, car parks, roads, pathways and grounds. The INMO's CCTV system is implemented in a proportionate manner as necessary to protect INMO property against theft, pilferage or damage, and for the safety and security of staff, members and visitors to our facilities (to protect their vital interests).

CCTV footage may only be monitored on the permission of the General Secretary, or her designate, and access to recorded footage is strictly limited to authorised personnel. Requests to access, and authorisation provided, will be recorded in writing and retained by the Data Protection Officer.

Footage is retained for 28 days, except where incidents or accidents have been identified in which case such footage is retained specifically in the context of an investigation of that issue.

CCTV footage may be used in the context of disciplinary proceedings involving INMO staff or members (to protect the vital interests of the INMO, staff, members and affected individuals). CCTV footage is not disclosed to third parties except where disclosure is required by law (such as for the purpose of preventing, detecting or investigating alleged offences) and in such instances disclosure is based on a valid request.

Signage indicating that CCTV is in use is displayed prominently.

5.13 Children's Personal Data

Children are identified in the GDPR as "vulnerable individuals" and deserving of "specific protection". Guidelines on the use of personal data relating to children are outlined in Appendix E.

6. Roles and Responsibilities

The Organisation has overall responsibility for ensuring compliance with the Data Protection Acts. However, all partners who process personal data in the course of their employment or work with the Organisation are also responsible for ensuring compliance with the Data Protection Acts.

The Organisation will provide support, assistance, advice and training to all relevant departments, offices and staff to ensure they are in a position to comply with the legislation. The Organisation's Data Protection Officer will assist the Organisation and its staff in complying with the Data Protection legislation.
Specifically, the following roles and responsibilities apply in relation to this Policy:

All users of Organisation information:

- Must complete relevant training and awareness activities provided by the Organisation to support compliance with this policy;
- Should take all necessary steps to ensure that no breaches of information security result from their actions;
- Must report all suspected and actual data security breaches to their head of department/function who must in turn report the incident immediately to the Data Protection Officer, so that appropriate action can be taken to minimise harm;
- Must inform the Organisation of any changes to the information that they have provided to the Organisation in connection with their employment (e.g. changes of address or bank account details).

Senior Management Team (SMT):

- the SMT is responsible for reviewing and approving this Policy as recommended by the General Secretary, or her designate;
- each member of SMT is responsible for ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility;

General Secretary:

The General Secretary is the Senior Officer within the INMO, with accountability for compliance with the Data Protection Acts and for:

- ensuring that this Policy is reviewed and approved by the UMTO as appropriate [check];
- ensuring that appropriate policies and procedures are in place to support this Policy;
- liaising with the SMT as appropriate;
- liaising with the Data Protection Officer as appropriate;
- ensuring that any data security breaches are properly dealt with.

The General Secretary may designate others to assist her in any or all of these functions, while retaining ultimate accountability.

Heads of Department, Function, Managerial Staff:

Heads of Department/Function/Managerial Staff are responsible for:

- ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility;
- nominating a suitable member of staff, where necessary, to be assist in coordinating Data Protection compliance matters within each of the areas under their remit;
- enabling the Data Protection Officer to maintain a record of processing activities by compiling, approving and returning the information required for the compilation of the Registers maintained by the Data Protection Officer.

Data Protection Officer:

The Data Protection Officer is responsible for administrative matters at an institutional level in relation to data protection. The principal data protection duties of the Data Protection Officer are to:

- process and respond to formal Data Access Requests;
- respond to requests for rectification, erasure of data and restrictions or objections to processing of data;
- initiate regular reviews of data protection policies and procedures and ensure documentation is updated as appropriate;
- provide advice to staff in relation to the completion of and outcome of Data Protection Impact Assessments;

- acting as the contact point for and cooperating/liaising with the Data Protection Commission where necessary/appropriate, including in the event of a data security breach;
- maintain a record of all personal data security breaches;
- organise targeted training and briefing sessions for INMO staff as required;
- provide advice and guidance to INMO staff on data protection matters;
- maintain a centrally-held register of the categories of personal data held by INMO;
- maintain records of INMO's compliance with the Data Protection Acts.

Staff, Executive Council Members, Local Representatives and other Partners of INMO:

All staff, executive council members, local representatives and other Partners are expected to:

- acquaint themselves with, and abide by, the rules of Data Protection set out in this Policy;
- read and understand this policy document;
- understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data;
- understand the lawful basis for processing personal data;
- not jeopardise individuals' rights or risk a contravention of the Act;
- report all data security breaches to their manager immediately;
- contact the Data Protection Officer if in any doubt.

7. Breach of this Policy

If any breach of this Policy is observed, then disciplinary action may be taken in accordance with the Organisation's disciplinary procedures (Relevant Policy and Rule Book) as amended or updated from time to time.

8. Supporting Policies, Procedures, Guidelines

This policy supports the provision of a structure to assist in the Organisation's compliance with the Data Protection Acts. The policy is not a definitive statement of Data Protection law. If you have any specific questions or concerns in relation to any matters pertaining to personal data, please contact the Organisation's Data Protection Officer.

The Policy should be read in conjunction with the following Organisation policies, procedures, and guidelines:

- APPENDIX G – INMO TYPES OF PERSONAL DATA, PROCESSING PURPOSE, AND LAWFUL BASES;
- APPENDIX H – DATA SUBJECT RIGHTS PROCEDURE
- APPENDIX I – DATA MANAGEMENT AND RETENTION POLICY
- APPENDIX J – DATA PROTECTION NOTICE FOR MEMBERS
- APPENDIX K – MEMBERSHIP APPLICATION PROCESS AND REVISIONS TO MEMBERSHIP FORM/ONLINE PORTAL
- APPENDIX L – WEBSITE DATA PROTECTION NOTICE

- APPENDIX M – WEBSITE COOKIES STATEMENT
- APPENDIX N – DATA BREACH PROCEDURE
- APPENDIX O – PROCEDURE WHEN PROVIDING MEMBERSHIP LISTS TO INMO REPRESENTATIVES
- APPENDIX P – SERVER/COMMS ROOM POLICY
- APPENDIX Q – POLICY FOR THE SECURE USE OF USB MEMORY DEVICES
- APPENDIX R – POLICY FOR INTERNAL MANAGEMENT OF DATA ACCESS REQUESTS
- APPENDIX S – STAFF DATA PROTECTION NOTICE
- APPENDIX T – CARD PAYMENT POLICIES AND PROCEDURES

9. Definitions

The Data Protection Acts govern the processing of personal data. As with any legislation, these and other terms used in the Data Protection Acts have a specific meaning. The following are some important definitions used in this policy, taken from the Data Protection Acts, with additional comments provided where appropriate:

Personal data

Personal data means information relating to-

a) an identified living individual

b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to

   i. an identifier such as a name, an identification number, location data or online identifier, or
   ii. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

This can be a very wide definition depending on the circumstances.

Special categories of personal data

Special categories of personal data (formerly known as "sensitive personal data") receive greater protection under the Data Protection Acts and refer to the following:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data or biometric data for the purpose of uniquely identifying a person;
- data concerning health;
- data concerning a person's sex life or sexual orientation

Data subjects have additional rights under Article 9 of the GDPR in relation to the processing of any such data.
Whilst criminal convictions and offences are not classed as special categories of personal data, the Data Protection Acts also provide additional rights to data subjects in this regard.

Data concerning health

Data concerning health means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual, that reveal information about the status of his or her health.

Data subject

Data subject is a living person who is the subject of personal data.

Data controller

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. INMO, for example, is a data controller in relation to personal data relating to its own staff and members.

Data owner

Data owner means the most senior person in the department/function within which the data is created. An exception can be made if this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area.

Data processor

Data processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller (Note: the term 'Data Processor' does not include an employee of a data controller who processes such data in the course of their employment. Examples of data processors include payroll companies, accountants and market research companies, all of which could hold or process personal information on behalf of someone else).

Direct marketing

Direct marketing is defined as:

- "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds.

The marketing must be directed to particular individuals. In practice, all relevant electronic messages (e.g. calls, faxes, texts and emails) are directed to someone, so they fall within this definition.

Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the rules apply.

An unsolicited message is any message that has not been specifically requested. So even if the member has 'opted in' to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the member agrees to future messages (and is likely to mean that the marketing complies with the Electronic Privacy Regulations) but this is not the same as someone specifically contacting you to ask for particular information.

Partners:

In this Policy, 'Partners' is used to refer to:

- any person who is employed or engaged by the Organisation who processes personal data in the course of their employment or engagement;
- any member of the Executive Council of the Organisation who processes personal data in the course of their duties;
- any local representative, in the meaning of our Rule Book, of the Organisation who processes personal data in the course of their studies;
- individuals who are not directly employed by the INMO, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the INMO.

Processing:

Processing is widely defined under the Data Protection Acts and means performing any operation or set of operations on personal data, whether or not by automated means, including-

1. the collection, recording, organisation, structuring or storing of the data,
2. the adaptation or alteration of the data,
3. the retrieval, consultation or use of the data,
4. the disclosure of the data by their transmission, dissemination or otherwise making the data available
5. the alignment or combination of the data, or
6. the restriction, erasure or destruction of the data.

Pseudonymisation

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. The Data Protection Acts still apply to personal data which has been pseudonymised.

10. Review

This policy has been approved by the General Secretary and Senior Management Team. Any additions or amendments to this or related policies will be considered by the Senior Management Team and must be approved by the General Secretary, or her designate.

The policy will be reviewed periodically, and at least annually, by the Data Protection Officer in light of any legislative or other relevant developments. The results of that review will in turn be considered by the Senior Management Team and the General Secretary, or her designate.

11. Further Information

If you have any queries in relation to this policy, please contact:

Data Protection Officer, INMO
Email: dataprotection@inmo.ie

12. Disclaimer

The Organisation reserves the right to amend or revoke this policy at any time without notice and in any manner in which the Organisation sees fit at the absolute discretion of the Organisation or the General Secretary of the Organisation.

APPENDIX A: LAWFUL BASES FOR PROCESSING (Article 6)

It is necessary under Article 6 of the GDPR to have a legal basis for processing ALL personal data. There are six legal bases set out in the legislation:

Consent from the individual

The individual must give consent at the outset. Inferred consent is not enough. Their consent must be freely given and the withdrawal of their consent should not have any adverse consequences for the individual.

Necessary for the performance of a contract

The contract must be between the controller and the data subject and the data must be necessary for the performance of that contract or necessary in order to take steps to enter a contract with the data subject. For example, processing data relating to an individual's qualifications and work history when considering entering into an employment contract.

Necessary for compliance with a legal obligation

INMO is required by statute to retain certain records, for example employment records, health & safety records, educational records.

Necessary to protect the vital interests of the individual or another natural person

This ground is applied in essentially "life and death" situations, for example where it is necessary to provide personal data to the emergency services in the case of an emergency situation.

Necessary for the performance of a task carried out in the public interest

This may occur where INMO carries out a task in the public interest or in an exercise where official authority has been invested in INMO as a data controller. However, a data subject can object to this lawful basis and challenge whether the processing is indeed in the public interest.

Necessary for the legitimate interests of the controller or a third party

The processing is necessary for INMO's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests and in the case of special categories of personal data, as covered by one of the lawful bases as set out in Article 9(1) of the GDPR, for example:

1. Explicit consent from the individual
2. Necessary for legal obligations of the controller as an employer insofar as it is authorised by EU or Irish law or a collective agreement
3. Necessary to protect the 'vital interests of the data subject where the data subject is physically or legally incapable of giving consent
4. Data has been 'manifestly made public' by the data subject themselves

5. Necessary for medical or health reasons subject to any applicable DPA measures and safeguards
6. Necessary for the ‘public interest’ subject to any applicable DPA measures and safeguards.

In the case of personal data relating to criminal convictions and offences, it must be covered by a lawful basis set out in the Acts.

If you have any questions in relation to the application of a lawful basis, please contact Organisation’s Data Protection Officer.

APPENDIX B: CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA (Article 9)

The GDPR sets out conditions for processing Special Categories of personal data. The Organisation must satisfy a lawful condition of processing personal data under Article 6 of the GDPR as well as one under Article 9 to process these categories of data.

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Personal data… may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

Note: There will are a number of additional grounds for processing 'special categories of personal data' (such as health data) under Irish law, in addition to those contained in Article 9 of the GDPR. Notably, these include a legal basis to process health data for insurance, pension or mortgage purposes.

APPENDIX C: CONDITIONS FOR PROCESSING PERSONAL DATA ABOUT CRIMINAL CONVICTIONS OR OFFENCES (Article 10)

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

The Data Protection Act deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.

APPENDIX D: CONDITIONS FOR CONSENT

Article 7 of the GDPR outlines the conditions for consent:

1. Where processing is based on consent, the Organisation must be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

APPENDIX E: GUIDELINES ON PROCESSING PERSONAL DATA RELATING TO CHILDREN

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

APPENDIX F: EXAMPLES OF PERSONAL DATA*

The following is a list of the types of data which would be considered to be 'Personal Data'. Please note: this list is not exhaustive.

People's names	Contact Details (incl. Home address, home phone/mobile nos., email addresses)
Date of Birth/Age	Birthplace/citizenship/nationality
Gender	Marital Status
PPS Numbers	Member/Staff Nos.
National ID Card details/Nos.	Next of kin / dependent / family details
Photographs	CVs
Personal financial data (e.g. Bank account details, DEBIT/CREDIT CARD DETAILS)	Details of gifts/donations made
Income / salary	Blood samples (linked to identifiable individuals)
Fingerprints/biometric data	CCTV images
Video images containing identifiable individuals	Voice recordings
Employment History	Sick leave details/medical certificates
Other leave data (excl. sick leave)	Qualifications/Education Details
Work performance	References for staff/interns etc
Grievance/Disciplinary Details	Examination/assignment results
Membership of Professional Associations	Signatures (incl. Electronic)

Passwords & PINS	Continuous Professional Development (CPD) records
Car registration details	Clinical files relating to research participants
Online identifiers (e.g. IP address)	Location data
Data relating to children	Research subject consent forms
SPECIAL CATEGORIES OF PERSONAL DATA:	
Racial or Ethnic origin	Biometric data for the purpose of uniquely identifying a natural person
Political opinions	Data Concerning health
Religious or philosophical beliefs	Data concerning a person's sex life or sexual orientation
Membership of a trade union	Genetic data
Data relating to the commission or alleged commission of any offence (incl. Garda vetting data)	**Any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings**

*While the Data Protection legislation only applies to data relating to LIVING individuals, due care and attention should also be given to personal/sensitive data relating to deceased individuals.

**Whilst criminal offences are no longer included in the definition of Special Categories of Personal Data, the collection and processing of criminal offence data is given special protection in the GDPR.

APPENDIX G: INMO TYPES OF PERSONAL DATA, PROCESSING PURPOSE, AND LAWFUL BASES.

Type of Personal Data	Purpose	GDPR Lawful Basis for Processing
Membership Database and Related Accounts Data		
• In relation to members – Name, contact details, date of birth, gender, bank/credit card/payroll details, place of work, payment history. • Records of contact with membership and accounts department.	Data is processed to: • Maintain a membership database to facilitate the provision of services to members across our industrial, professional and regulatory functions in furtherance of our contract with them; • Facilitate the administration of INMO functions in relation to accounting obligations, financial administration, and the fulfilment of our legal obligations; • Facilitate, where necessary, our legal obligations in the conduct of lawful ballots for industrial action; • Facilitate communication with our members on matters of concern to them in fulfilment of our contract with them; • Facilitate the identification and recruitment of non-members in individual workplaces; • Facilitate the provision of valued added services and opportunities to our members by other organisations. • Facilitate payments for membership and other services and events.	Necessary for performance of a contract under Art. 6(1)(b) GDPR; and Performance of legitimate activities by non-profit body with a trade union aim under Art. 9(2)(d) GDPR; and Contract performance Art. 6(1)(b) GDPR; and Consent under Article 6(1)(a).

Photographs and Videos of Members		
• Photographs and videos at events and functions associated with the INMO.	Data is processed to: • Facilitate dissemination of information of interest to members; • Facilitate the advancement of the collective aims of the members of INMO;	Consent under Article 6(1)(a); Performance of legitimate activities by non-profit body with a trade union aim under Art. 9(2)(d) GDPR.
Records of Senior Managerial, Information, Industrial and Regulatory Departments		
• Records generated in seeking industrial advice; • Records generated in seeking professional advice; • Records generated in seeking advice on a regulatory matter; • Records generated in seeking advice on a legal matter; • Records generated in seeking advice on an indemnity matter; • Records generated in contacting a department of the INMO in relation to the activities of the INMO in a particular workplace or in relation to a particular issue; • Records generated arising from meetings of members, or with members, including, but not limited to; Executive Council Meetings, Meetings of Committees of the Executive Council; Meetings of Branches; Meetings of Professional Sections and Meetings of or with a member or members in any location; • Records generated in the course of the administration of functions provided for under the INMO Rule Book in relation to the relationship between members *inter se*	Data is processed to: • Facilitate the provision of services to members across our industrial, professional and regulatory functions in furtherance of our contract with them; • Facilitate our ethical and legal obligations to maintain records of discussions, deliberations, advice and actions; • Facilitate the administration of the relationship between members *inter se* and between the Organisation and its members; • Facilitate the defence of legal actions against the Organisation; • Facilitate the recording and verification of educational attainment;	Performance of legitimate activities by non-profit body with a trade union aim under Art. 9(2)(d) GDPR; and Contract performance under Art. 6(1)(b) GDPR; and Necessary for the establishment, exercise or defence of legal claims under Art. 9(2)(f) GDPR; see also Sections 46 and 47 and more generally Part 2, Chapter 2 Data Protection Act 2018.

and between the Organisation and its members; • Records generated in the course of consultations, meetings, investigations, hearings, including employment, regulatory and third party processes and hearings where the INMO has been requested to provide advice, or in turn provides assistance; • Records of attendance at professional courses, conferences and meetings; • Records of achievement and related records concerning completion of educational courses.		
Visitors		
• Conference Attendees; • Meeting Attendees; • Other visitors.	• Administration of conferences; • Administration of meetings; and • CCTV surveillance of INMO premises.	Contract performance under Art. 6(1)(b) GDPR; and Consent under Article 6(1)(a); and Protecting the vital interests of employees and other persons (Art 6(1)(d)).
Employees		
• See internal Staff Data Protection Notice	• See internal Staff Data Protection Notice	See internal Staff Data Protection Notice
Suppliers, Contractors and Business Contacts		
• Name, contact details of suppliers, contractors and business contacts; • Personal Data relevant to performance of contract.	• Performance of services / supply of goods	Consent under Article 6(1)(a); and Necessary for the purposes of the legitimate interests pursued by INMO under Art. 6(1)(f); and

		Contract performance under Art. 6(1)(b) GDPR.
Health Screening Data related to Covid-19		
• Name, contact details of employees, and all other visitors to INMO offices • Personal Data related to health, as recommended by national health authorities and the Government for the purposes of managing business operations in the context of Covid-19.	• Allow continuation of business activities in the context of Covid-19, and to manage activities to assist in controlling the spread of the virus as recommended by national health authorities and the Government.	Consent under Article 6(1)(a); and Protecting the vital interests of employees and other persons (Art 6(1)(d)); Necessary for the purposes of the legitimate interests pursued by INMO under Art. 6(1)(f); and Necessary for a task carried out in the public interest (Art. 6(1)(e).

APPENDIX H – DATA SUBJECT RIGHTS PROCEDURE

1. Introduction

Your privacy and data protection rights are important to INMO. As described in the INMO Privacy Policy, there are a number of rights which you may exercise under data protection law. This guide explains what these rights are and how to exercise them. Capitalised terms in this document are defined in the INMO Privacy Policy.

2. What are your rights?

RIGHT	DESCRIPTION
Inspection and access	Allows you to request a summary and/or a copy of your Personal Data which we Process or which is Processed on our behalf together with details about the way in which we Process your Personal Data.
Rectification	Allows you to request that any inaccurate Personal Data be rectified.
Erasure (right to be forgotten)	In certain circumstances, allows you to request that Personal Data be deleted.
Restriction	Allows you to request that Processing of your Personal Data by INMO be restricted.
Portability	Allows you to request that INMO transmit certain Personal Data that you have provided to INMO either to you or to another Controller.
Objection	Allows you to object based on your particular circumstances to data Processing being carried out by INMO, in which case INMO have to stop such Processing.
Automated decision- making	You have a right not to be subject to certain forms of automated decision-making if the decision produces legal effects or similarly significantly affects you and where there is no human input involved. INMO will seldom, if ever, undertake such activities.

However, please note that these rights are available to individuals' subject to certain criteria as set out in data protection legislation and therefore will not be available in all circumstances.
Exceptions to the right of access
The Data Protection Act 2018 sets out some limited circumstances in which an organisation may not be required to provide you with a copy of your personal data. In particular, an organisation may be exempt from providing you with personal data if a restriction of your right of access is necessary:

- in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure
- for the enforcement of civil law claims, including matters relating to any liability of an organisation in respect of damages, compensation or other liabilities or debts related to the claim.

In addition, an organisation may not be required to provide you with a copy of your personal data where the data consists of an expression of opinion about you by another person given in

confidence, or on the understanding that it would be treated as confidential, to a person who has a legitimate interest in receiving the information.

An individual's right of access may also be restricted where, in the opinion of a medical professional, to grant access to the data would be likely to cause serious harm to the individual's physical or mental health. Access to personal data kept for, or obtained in the course of, carrying out of social work by a public authority, public body, voluntary organisation or other body may be similarly restricted.

Access to personal data may also be restricted where such restrictions are necessary for the purposes of safeguarding important objectives of public interest.

Finally, the GDPR also provides that the right to obtain a copy of your personal data must not adversely affect the rights and freedoms of others. For example, when responding to an access request, an organisation should not provide the requestor with personal data relating to a third party that would reveal the third party's identity.

3. Exercising Your Rights

You may exercise the rights set out above by contacting the INMO Data Protection Officer: by email at data.protection@INMO.ie or by post to Data Protection Officer, INMO, North Brunswick Street, Dublin 7.

To help us to respond to your request, please be as specific as possible. For example, if you wish to exercise your right to access your Personal Data, please specify the Personal Data of which you wish to obtain a copy. Please include any additional details that would help us to respond to your request - for example, a staff reference number, names of INMO Departments/Offices that you were associated with, etc.

If you wish a third party to submit a request to exercise your rights on your behalf (e.g. a family member or solicitor), you must provide written authorisation to allow us to disclose your Personal Data to that third party.

You may be asked to provide proof of identity. Acceptable forms of identification include: copy of passport, driving licence or staff ID card. Copies are acceptable in most cases; however, we reserve the right to ask to see original documents where necessary. Copies of such documents will be securely destroyed once we have verified your identity.

In the normal course of events, we are obliged to respond to your access request within one month of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). Where we are extending the period for replying to your request, we must inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.

There is no fee payable by you to make an access request. However, where we believe a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the organisation may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s).

4. Right to Complain

If we do not comply with a valid access request that you have made, or if you have another complaint in relation to our Data Protection processes, it is open to you to make a complaint to the Data Protection Commissioner.

The Data Protection Commissioner recommends that you contact us to establish the circumstances and to indicate your intention to complain to their Office, prior to doing so. Indeed, by doing so we may be in a position to correct the problem there and then.

If, having contacted us directly, you are not satisfied with our response, you may wish to raise a concern with the Data Protection Commissioner, a complaint may be made online by visiting https://www.dataprotection.ie.

For more information about your rights to information and access under the GDPR, please see the following link: http://gdprandyou.ie/gdpr-for-individuals.

APPENDIX I – DATA MANAGEMENT AND RETENTION POLICY

1. Purpose

This is the data and document Management and Retention Policy ("Management and Retention Policy") of the Irish Nurses and Midwives Organisation ("the INMO"). This Policy applies to INMO, which includes all partners identified in the Data Protection Policy and contractors engaged by INMO (together "INMO partners"). The purpose of this Policy is to state INMO's policy concerning the management, retention and destruction of Personal Data (e.g. documents, records, emails and correspondence, files, audio visual files and recordings and any other forms of information and records regardless of their format together referred to as "Data").

2. Management and Retention principles

Having regard to the principles contained in Article 5(1) of the General Data Protection Regulation (EU No. 2016/679) ("GDPR"), it is the policy of INMO to:

a) retain personal data in identifiable form only for such period as is necessary in relation to the purpose for which the data are processed (the "storage limitation" principle);
b) ensure that personal data retained by INMO is adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed (the "data minimisation" principle);
c) take all reasonable measures to ensure that personal data retained by INMO are accurate (the "accuracy" principle); and
d) ensure that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Having further regard to the principles contained in Article 32 of the General Data Protection Regulation (EU No. 2016/679) ("GDPR"), it is the policy of INMO to:

1. Take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and in so doing implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
    a. the pseudonymisation and encryption of personal data;
    b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Further, we shall take steps to ensure that any natural person acting under our authority who has access to personal data does not process them except on instructions from the us, unless required to do so by law.

3. INMO Activities

Having regard to Article 24 of the GDPR, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the INMO shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

The suite of policies relating to data protection aim to achieve this objective, and this policy further takes specific account of the principles at 2 above.

As set out in the Appendix G to the Data Protection Policy and Appendix B to the Staff Data Protection Notice the INMO has a lawful basis to undertake data processing, including the retention of personal data. Accordingly, it is the policy of INMO to retain and hold personal data in performing its functions in a manner that is consistent with the principles of storage limitation, data minimisation, accuracy integrity, and confidentiality.

4. Application of this Policy

This Policy applies to any type of Data created, received, transmitted and retained in the context of INMO's day to day activities in performance of its functions and any other data processing undertaken by INMO, regardless of the format.

Therefore, any paper records or electronic files that are part of any of the categories listed in Appendix G to the Data Protection Policy and Appendix B to the Staff Data Protection Notice must be retained for the period listed in this policy.

Data should not be retained beyond the period indicated in the this policy, unless a valid operational reason (or a litigation hold or other exceptional situation) calls for its continued retention. If you are unsure whether to retain a certain record, please contact the Data Protection Officer.

5. Data Ownership

All Data, irrespective of format, generated, created, received and/or retained by INMO in performing the INMO's functions is the property of the INMO and subject to its overall control. INMO Personnel leaving INMO or changing positions within INMO are not to remove any Data without the prior written authorisation of their Department/Unit Head.

6. Data Management and Storage

INMO's records must be stored in a safe, secure and accessible manner to ensure the security and confidentiality of such Data in accordance with INMO's Data Protection Policy.

6.1 Guidance in Relation to Integrity and Confidentiality in the Storage and Management of Personal Data

INMO's records must be stored in a safe, secure and accessible manner to ensure the integrity, security and confidentiality of such Data.

Special care is to be taken to ensure that information of a sensitive nature, in particular, information that constitutes a special category of personal data under the GDPR, is stored in a secure manner which may include, for example, locked filing cabinets and offices for hard copy Data and/or the use of password protection and encrypted files for Data stored in electronic form.

The following sections are important standards to ensure the integrity and confidentiality of the data we process.

6.1.1 Personal data should not be deliberately or inadvertently viewed by uninvolved parties:

- Staff should operate a clear desk policy at the end of each working day and when away from the desk or the office for long periods. If a clear desk policy is not possible then access restriction must be implemented.
- Personal and sensitive records held on paper and/or on screens must be kept hidden from callers to offices.
- Records containing personal information must never be left unattended where they are visible or maybe accessed by unauthorised staff or members of the public.
- If computers or VDUs are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public.
- The use of secured screen savers is advised to reduce the chance of casual observation.
- Rooms, cabinets or drawers in which personal records are stored should be locked when
- unattended. If locked cabinets are not possible, then access control to the room should be introduced.
- It is important to ensure that member/or staff information is not discussed in inappropriate areas where it is likely to be overheard including conversations and telephone calls. Particular care should be taken in areas where the public have access.
- While appreciating the need for information to be accessible, staff must ensure that personal records are not left on desks or workstations at times when unauthorised access might take place.
- Staff must only access member information on a need to know basis and should only view or share data that is relevant or necessary for them to carry out their duties.

6.1.2 Do not leave information/data unattended in cars:

- Staff must not leave laptops/portable electronic devices and/or files containing personal information unattended in cars.
- In cases where staff removes files/records from offices to attend meetings, or as necessary to consult with or provide services to members the records should always be contained in a suitable brief case/bag to avoid any inappropriate viewing and also to secure the records.

- All files and portable equipment must be stored securely. If files containing personal data must be transported in a car, they should be locked securely in the boot for the minimum period necessary.
- Staff should not take records containing personal data home, however, it is recognised that this is exceptionally necessary for the purposes of staff who work in the field. Thus, where this cannot be avoided the records must be stored securely. Records should not be left in a car overnight but stored securely indoors.

6.1.3 Transmitting information by Fax or Post

- Staff must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid work related reason.
- If a staff member receives a fax message and they are not the intended recipient they must contact the sender and notify them of the error.
- Fax machines must be physically secured and positioned to minimise the risk of unauthorised individuals accessing the equipment or viewing incoming messages.
- Where possible the information should be encrypted and transmitted via email.

It is acceptable to transmit confidential and personal information by fax only when:

1. All persons identified in the fax message have fully understood the risks and agreed.
2. There are no other means available.

The following steps are to be taken to maintain security and confidentiality when transmitting personal information by fax:

- The fax message must include an INMO fax cover sheet.
- Only the minimum amount of information necessary should be included in the fax message.
- Before sending the fax message, contact the intended recipient to ensure he/she is available to receive the fax at an agreed time.
- Ensure that the correct number is dialled.
- Keep a copy of the transmission slip and confirm receipt of the fax message.
- Ensure that no copies of the fax message are left on the fax machine.

When using the postal system, mail containing sensitive personal information should be marked clearly with "Strictly Private and Confidential". If proof of delivery is necessary, information of this nature should be sent by registered post. Please also provide “return to sender” information in the event that the mail is undeliverable.

Additional issues when using the postal system:

1. When ascertaining the address of a member to whom information containing personal data is being posted please bear in mind that there may be multiple persons with the same name, and similar address or work location, within our membership system;
2. If accessing an address via the membership database – prior to finalising the address to which the correspondence will be sent cross check the information from the database with the file in question to ensure the material is being sent to the correct member.

6.1.4 Transmitting information by Email

Email represents an important, and ever more frequently the predominant, means of communication with our members and others with whom we interact. Email, in and of itself, is not a secure form of communication, and therefore:

1. Emails may be used to communicate with members and others;
2. However, care must be taken in relation to the contents of email;
3. While an email in itself represents a form of personal data, insofar as a person can be identified from the address, it is the confidentiality and integrity of the information to be communicated which is of paramount concern;
4. If any information is to be communicated which contains personal data (particularly confidential, sensitive, or special category data) and which if viewed by others would represent a breach of confidentiality then the information should be included in an attachment to the email which is password protected, and thus encrypted. This includes word documents, PDFs and other forms of documents.
5. Personal data, particularly confidential, sensitive, or special category data, must not be included in the body of an email.
6. The password for the encrypted files should be sent via a separate email to the recipient.
7. Caution must be exercised in sending email generally to ensure that the address entered is the address of the intended recipient bearing in minding similar names and email addresses.

6.1.5 Electronic Storage of Data (Laptops, Mobile Phones, Tablets, Mobile Storage Devices)

All portable data, and in particular personal data, must be stored on/accessible via encrypted devices and drives only, using methods recommended by the IT Department.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar. Devices are not to be left in vehicles while the vehicle is unattended.

Electronic Measures:

- Access to the computer's operating system and company software will be password protected.
- A user registration and removal policy will be in place.
- Appropriate internet security software will be installed and maintained.
- A robust backup procedure will be implemented so that if data is corrupted or lost, a recent copy of the electronic records will be available.
- Security updates and software patches will be regularly installed.
- There will be an audit trail of which records have been accessed by different users of the system. this aims to allow the data controller to ensure that records are not being accessed inappropriately.
- All persons must adhere to the Password Standard as issued from time to time by the IT department – which will include advice as to the frequency of password change, format of password and related matters. The password to your device, or for access to any element of our IT systems, must not be shared with any person, other than a member of the IT department or another person who is authorised to access the data stored on or accessible via your device.

Regarding Mobile Devices with apps such as Outlook which can retrieve emails and Organizational information on a personal mobile device and provide remote access.

1. Personal mobile devices which download any INMO content including emails/attachments or any other INMO information must be password protected.

2. User must delete any content from the device as soon as permission is withdrawn to utilise an INMO account, or before the device is given to another person or for any other reason which could result in unauthorized access to INMO generated emails / information considered confidential and for INMO use only.

Other points re IT infrastructure:

- Access to computer servers should be restricted and should not be accessible with due controls being in place.
- Computer servers should be kept in cool well-ventilated rooms and fitted with surge protectors and an auxiliary power supply to prevent data loss due to power surges or failure.
- When disposing of obsolete or redundant equipment many data controllers offer the equipment for sale to staff or donate it to charities. It is the responsibility of the data controller to ensure that all data previously stored on the devices has been removed prior to disposal. it is not sufficient to merely reformat the hard drives of the devices, as data can still be retrieved. Software is available that will overwrite the contents of the hard drive with a series of 1's and 0's to ensure that previous data cannot be retrieved. Dependant on the nature of the data stored, it is recommended that hard drives should be overwritten between three and five times.

Use of SMS Messaging:

- The use of text or SMS messages to personnel can appear an efficient and attractive way of communicating with members/employees/employers etc.
- There are difficulties however with sending confidential information in this way as text messages can be read by others and mobile phone numbers can change.
- It is advisable therefore to restrict messages by text to non-personal matters such as appointment reminders or notifications.
- Personal consent is required in order to communicate personal information with clients or employees by means of text messages.

The IT Department will from time to time issue further guidance in relation to the security of IT systems, desktop devices, tablets, and mobile devices (including mobile phones). Such guidance is in furtherance of compliance with our obligations pursuant to the GDPR and related legislation and should be regarded as forming part of both this Policy and the Data Protection Policy for the Organisation, and should be regarded as such by all concerned. Any such guidance shall make reference to the appropriate data protection policies.

6.1.6 Card Payment Policies and Procedures

Appendix T contains guidance in relation to staff who are authorised to facilitate debit or credit card payments.

The processing of such payments using an online portal or terminal potentially engages data protection concerns and it is imperative that all aspects of the policy and procedures are adhered to at all times.

6.2 Destruction of Data

Once Data have met their required retention period in accordance with the principles set out in this Policy, such Data should then be deleted or destroyed or anonymized as follows:

a) Hard copy files: to be destroyed by confidential shredding or by using the services of an approved confidential waste disposal firm.
b) Electronic files: to be purged or deleted or anonymized from all relevant systems on which such Data is stored and/or data bases. The destruction of electronic records must be coordinated with the IT Department.
c) Data stored in other media: to be deleted or destroyed or anonymized in a safe and confidential manner to ensure the content is not disclosed.
d) In relation to INMO Representatives or Members of Executive Council, on their resignation or cessation of office, they are requested to return or where appropriate securely delete/destroy any personal data held by them. If we are notified of the death or incapacity of an INMO Representative or Member of Executive Council, we will communicate with the Estate of that individual requesting the return or where appropriate secure deletion/destruction of any personal data held by the person who held the data.

7. Litigation or Other Hold

INMO requires all INMO Personnel to fully comply with the general guidance set out in this Policy and the specific retention periods set out herein. However, all INMO Personnel should note the following general exception to any stated destruction schedule: if you believe, or your Department Head/Senior Manager informs you, that certain Data held by INMO is relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit or other event, you must preserve and not delete, dispose, destroy or change such Data, including e-mails, until advised that such Data is no longer needed. This exception is referred to as a "Litigation Hold", and takes priority over any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact the Data Protection Officer.

8. Compliance with this Policy

It is the responsibility of each INMO Department/Unit to ensure that personal data is retained by that Department/Unit in compliance with this Policy and to ensure that all INMO Personnel under their responsibility comply with this Policy. Operational responsibility rests with each Department Head.

In turn all staff have an obligation to familiarise themselves with the contents of this policy and to abide by its contents where relevant to their work.

ANNEX 1 – Retention Schedule

INMO is committed to its obligations under the General Data Protection Regulation (GDPR). This Policy sets out our position in respect of the principle that data not be retained for longer than reasonably necessary. The below schedules set out the statutory data retention / record keeping periods to which INMO must comply. In order to ensure that we are capable of supporting data access requests or fulfilling other statutory obligations, it is INMO policy to retain data for an additional 12 months after the expiry of the statutory record- keeping period.

Staff Records

Record	Retention Period	Justification for time frame
Benefits descriptions per employee	Permanent	Irish employment law and for pension calculation and record keeping
Employee applications and resumes	6 years or where successful, for the duration of the employment plus 7 years from the date of termination of employment	Section 11 of The Statute of Limitations Act 1957[1]
Employee benefit plans	6 years from when the record was required to be disclosed save pension detail requirements	Benefit of the employee
Employee offer letters (and other documentation regarding hiring, promotion, demotion, transfer, termination or selection for training)	6 years from date of making record or action involved, whichever is later, or 1 year from date of involuntary termination	Benefit of the employee Statute of Limitations
Records relating to background checks on employees	6 years from when the background check is conducted	Statute of Limitations
Employment contracts; employment and termination agreements	7 years from the date of expiry of the contract or agreement	Benefit of the employee Statute of Limitations
Employee records with information on pay rate or weekly compensation	3 years	Benefit of the employee Statute of Limitations
Tax forms	6 years after date of hire	Revenue obligation
Injury and Illness Incident Reports and related Annual Summaries; Logs of work-related injuries and illnesses	6 years following the end of the calendar year that these records cover	Statute of Limitations

[1] Note – references to the Statute of Limitations throughout this Annex, while referring to the Act of 1957, may also be taken to refer to the periods of time provided for in employment rights legislation in relation to wrongs, a remedy and applicable timeframes.

Supplemental record for each occupational injury or illness; Log and Summary of Occupational Injuries and Illnesses	6 years following the year to which they relate	Statute of Limitations
Job descriptions, performance goals and reviews; garnishment records	For the duration of the employment plus 7 years from the date of termination of employment	Benefit of employee Statute of Limitations
Employee tax records	6 years from the date tax is due or paid	Revenue obligations
Medical exams required by law	Duration of employment + 30 years	Benefit of employee
Personnel or employment records	6 years from the date the record was made, or 2 years from date of termination depending on the nature of the record.	Benefit of employee Statute of Limitations
Pension plan and retirement records	Permanent	Benefit of employee
Pre-employment tests and test results	2 years from date of termination	Benefit of employee Statute of Limitations
Salary schedules; ranges for each job description	2 years	Benefit of employee Statute of Limitations
Time reports	Termination + 3 years	Benefit of employee Statute of Limitations
Training agreements, summaries of applicants' qualifications, job criteria, interview records	Duration of training + 4 years	Benefit of employee

Payroll Records

Record	**Retention Period**	**Justification for time frame**
Payroll registers (gross and net)	3 years from the last date of entry	Benefit of employee Statute of Limitations
Time cards; piece work tickets; wage rate tables; pay rates; work and time schedules; earnings records; records of additions to or deductions from wages; records on which wage computations are based	7 years	Benefit of employee Statute of Limitations

Prospective employees

Record	Retention Period	Justification for time frame
Curriculum vitae	2 years	For future employment opportunities
Interview notes	2 years	For future employment opportunities Statute of Limitations

CCTV

Record	Retention Period	Justification for time frame
CCTV recordings	28 days	Security purposes

Accounting and Finance

Record	Retention Period	Justification for time frame
Accounts Payable and Receivables ledgers and schedules	7 years	Revenue Requirements
Annual audit reports and financial statements	Permanent	Good Governance, Revenue and Legislative Requirements
Annual plans and budgets	2 years	Good Governance, Revenue and Legislative Requirements
Bank statements, cancelled checks, deposit slips	7 years	Good Governance, Revenue and Legislative Requirements
Business expense records	7 years	Good Governance, Revenue and Legislative Requirements
Cash receipts	2 years	Good Governance, Revenue and Legislative Requirements
Details of cheques/stubs	7 years	Good Governance, Revenue and Legislative Requirements
Electronic fund transfer documents	7 years	Good Governance, Revenue and Legislative Requirements
Employee expense reports	7 years	Good Governance, Revenue and Legislative Requirements

General ledgers	Permanent	Good Governance, Revenue and Legislative Requirements
Journal entries	7 years	Good Governance, Revenue and Legislative Requirements
Invoices	7 years	Good Governance, Revenue and Legislative Requirements
Petty cash vouchers	3 years	Good Governance, Revenue and Legislative Requirements
Credit/Debit Card Merchant Receipts	7 years	Good Governance, Revenue and Legislative Requirements
Credit/Debit Card – additional data as per Appendix T	Limited authorised retention for regulative, legislative, or operational reasons – for the period required to discharge those obligations.	Good Governance, Revenue and Legislative Requirements

Tax Records

Record	Retention Period	Justification for time frame
All tax records	7 years	Good Governance, Revenue and Legislative Requirements

Legal and Insurance Records

Record	Retention Period	Justification for time frame
Appraisals	6 years from termination	Statute of limitations
Insurance claims/ applications	Permanent	Good governance
Insurance disbursements and denials	Permanent	Good governance
Insurance contracts and policies (Director and Officers, General Liability, Property, Workers' Compensation)	Permanent	Good governance
Leases	6 years after expiration	Statute of Limitations
Real estate documents (including loan and mortgage contract, deeds)	Permanent	Good governance

Membership Database and Related Records

Record	Retention Period	Justification for time frame
Membership Database Details i.e. membership record relating to membership history	45 years	Benefit of Member, Facilitation of service provision, Statute of Limitations
Accounting data relating to membership, membership services, or disbursements	7 years	Benefit of Member, Good Governance, Revenue, Statute of Limitations
Records generated in seeking industrial advice; Records generated in seeking professional advice; Records generated in seeking advice on a regulatory matter; Records generated in seeking advice on a legal matter; Records generated in seeking advice on an indemnity matter; Records generated in contacting a department of the INMO in relation to the activities of the INMO in a particular workplace or in relation to a particular issue; Records generated in the course of the administration of functions provided for under the INMO Rule Book in relation to the relationship between members inter se and between the Organisation and its members; Records generated in the course of consultations, meetings, investigations, hearings, including	7 years from the conclusion of the matter, or the INMOs involvement in the matter, in question	Benefit of Member, Good governance, Statute of Limitations

employment, regulatory and third party processes and hearings where the INMO has been requested to provide advice, or in turn provides assistance; Records generated in the course of the administration of functions provided for under the INMO Rule Book in relation to the relationship between members *inter se* and between the Organisation and its members;		
Records generated arising from meetings of members, or with members, including, but not limited to; Executive Council Meetings, Meetings of Committees of the Executive Council; Meetings of Branches; Meetings of Professional Sections and Meetings of or with a member or members in any location; Records of attendance at professional courses, conferences and meetings;	Executive Council Minutes – Permanent Branch, Professional Section, group/individual member meetings – 7 years Conference/Course attendance – 2 years	Good governance, legal obligations, historical record Benefit of Member, Good governance, Statute of Limitations Benefit of Member, Good Governance, Verification of Educational attainment.
Records of achievement and related records concerning completion of educational courses.	Permanent	Benefit of Member, Verification of educational attainment
Name, contact details of suppliers, contractors and business contacts;	Two years from termination of relationship	Benefit of Data Subject, Future business relationship
General contracts – for breach of contracts claims.	7 years	Statute of Limitations

Covid-19 Declaration Form

Record	Retention Period	Justification for time frame
Employee/Visitor Covid-19 Declaration Form	14 days from submission.	To facilitate contact tracing with public health authorities.

Exceptional Cases – Objective Justification

There may be times when the INMO needs to retain personal data for a longer period than either the time set out in law or the retention period set out above. Where this is the case, there will always be an objectively justifiable reason for keeping the data outside the normal period. This justification will be documented and held with the data concerned. In accordance with the principle of 'data minimisation', only the records needed will be retained and any and all ancillary data will be disposed of in accordance with INMO's Data Protection Policy and Guidelines and in taking all reasonable precautions in compliance with our GDPR obligations.

APPENDIX J – DATA PROTECTION NOTICE FOR MEMBERS

Irish Nurses and Midwives Organisation Data Protection Notice for Members[2]

Data Privacy

The Irish Nurses and Midwives Organisation collects and processes personal data relating to its members in the course of our work. We collect and process this data in order to provide you with services and to administer your Organisation effectively and in accordance with our legislative obligations. Additionally, members of the Organisation engage with us in relation to a wide range of issues, of often a sensitive nature, relating to their employment and they do so on the basis of the confidential nature of the service we provide. Therefore, they have a reasonable expectation of privacy and confidentially when engaging with the Organisation in matters relating to their employment and the data associated with such engagement.

As an Organisation we take your right to data privacy and control seriously and this notice will direct you to information in relation to what data we collect, why we collect, how it is processed, how long we will retain the data and importantly your rights in relation to the data.

What information do we collect and why, and how to we process that information?

As an Organisation we collect and process personal data to provide you with services and to effectively administer your Organisation.

We have compiled a list of data we collect, why it is collected, and our legal bases for processing the data. This list is available at APPENDIX G of the Data Protection Policy. Further details in relation to the legal bases for processing data can be found in the body of the Data Protection Policy.

Where we process your data on the basis of consent, e.g. direct marketing by partner companies for the provision of value added services, you have the right to withdraw that consent at any time. You can do so by contacting our membership department at membership@inmo.ie.

Who do we pass your information to?

We will occasionally, in the course of providing industrial, professional, or regulatory services to you, pass your information to legal advisors and insurers who are assisting us in providing services to you.

In the course of providing professional services to you, e.g. access to educational databases maintained by other professional organisations, it may be necessary to pass minimal personal data to those organisations, however, you will be specifically asked to consent to this process, and you may withdraw consent at any time.

[2] This document must be made available as a separate document in the data protection section of our website, reference must be made to the document in our membership application paper form and in the online application system, and a copy must be sent to each new member.

In the course of providing value added services we may pass personal data to companies or brokers carefully selected by the Executive Council, who in turn may contact you to offer you such value added services. As this constitutes Direct Marketing, when you enter into membership you will be asked to consent to this process, and you may withdraw consent at any time.

We may transfer personal data to a contractor in the United Kingdom, which is outside European Economic Area (EEA). This occurs on the basis of an adequacy decision issued under the GDPR by the EU Commission on 28 June 2021 which determined that personal data can flow freely from the European Union to the United Kingdom where it benefits from an essentially equivalent level of protection to that guaranteed under EU law.

How long will we retain your data?

We have compiled a list of data we collect, security provisions in relation to processing, and the proposed retention period. This list is available at APPENDIX I of the Data Protection Policy.

Automated Decision Making and Profiling?

We do not use automated decision making or profiling in the course of our activities.

What are your rights?

Data Protection legislation provides you with a range of rights in relation to access and controlling the processing of your data.

In brief, those rights include:

- The Right to be Informed
- The Right of Access
- The Right to Rectification
- The Right to Erasure
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object

These rights apply to varying degrees depending on the circumstances, and full explanation of these rights is contained in section 5.6 of the Data Protection Policy.

To access any of these rights free of charge, or to make further enquiries, please contact our Data Protection Officer at dataprotection@inmo.ie, or by writing to the Data Protection Officer, Irish Nurses and Midwives Organisation, North Brunswick Street, Dublin 7.

Please see APPENDIX H of the Data Protection Policy where you will find our Data Subject Rights Procedure.

Complaints

If you believe we have contravened Data Protection Legislation or any aspects of our Data Protection Policy please contact our Data Protection Officer at dataprotection@inmo.ie, or by writing to the Data Protection Officer, Irish Nurses and Midwives Organisation, North Brunswick Street, Dublin 7. We will endeavour to address the situation to your satisfaction.

If we do not comply with a valid access request that you have made, or if you have another complaint in relation to our Data Protection processes, it is open to you to make a complaint to the Data Protection Commissioner.

The Data Protection Commissioner recommends that you contact us to establish the circumstances and to indicate your intention to complain to their Office, prior to doing so. Indeed, by doing so we may be in a position to correct the problem there and then.

If, having contacted us directly, you are not satisfied with our response, you may wish to raise a concern with the Data Protection Commissioner, a complaint may be made online by visiting https://www.dataprotection.ie.

For more information about your rights to information and access under the GDPR, please see the following link: http://gdprandyou.ie/gdpr-for-individuals.

Further information is also available at APPENDIX H of the Data Protection Policy where you will find our Data Subject Rights Procedure.

APPENDIX K – MEMBERSHIP APPLICATION PROCESS AND REVISIONS TO MEMBERSHIP FORM/ONLINE PORTAL

Membership Application Process

In the course of facilitating an application for membership the following must occur, as well as other processes:

1. The relevant form, online portal, must contain the text set out below.
2. A copy of Data Protection Notice for Members must be sent to each new member.

Revised Text Membership Applications

1. Text for inclusion within membership form/online membership portal re Data Protection Generally

The Irish Nurses and Midwives Organisation ('the INMO') collects and processes personal data arising from your membership and in the course of providing services to you. INMO's Data Protection Notice for Members, and Data Protection Policy, is available at www.inmo.ie/dataprotection, and provides you with full details about how we process your personal data. It also provides you with important information regarding your rights in relation to the personal data we hold about you and how you can exercise those rights.

2. Additional Material for inclusion within membership form/online membership portal re Direct Marketing

The Executive Council of the INMO carefully selects companies and brokers who are in a position to offer you value added services arising from your membership.

Don't miss out on this valuable benefit of INMO membership! Tick here to allow our partners to contact you about value added services [Box]

INMO will provide partners with limited personal information you have provided us, i.e. contact details, to allow our partners use information you have provided here to contact you to offer you these value added services. INMO will share your information where you have ticked the box to join. You can instruct us at any time to no longer share your details by emailing membership@inmo.ie.

APPENDIX L – WEBSITE DATA PROTECTION NOTICE

Irish Nurses and Midwives Organisation
Website Data Protection Notice

This statement relates to the Irish Nurses and Midwives Organisation's privacy practices in connection with our websites. The Organisation is not responsible for the content or privacy practices of other websites. External links to other websites are not always clearly identifiable as such. Within the Organisation domain you may find websites over which the Organisation has no editorial responsibility or control. Such sites can include the websites of other organisations etc.

General statement

INMO fully respects your right to privacy and actively seeks to preserve the privacy rights of those who share information with the Organisation. The Organisation will not collect any personal information about you on this website without your permission save in cases where the Organisation is required by law to do so (e.g. the investigation of a criminal offence or a breach of the Organisation's policies, procedures or guidelines). Any personal information which you volunteer to the Organisation will be treated with the highest standards of security and confidentiality, in accordance with the GDPR, and Data Protection Acts 1988 to 2018. The Organisation's Data Protection Policy, available at www.inmo.ie/dataprotection, documents the Organisation's application of the Data Protection Principles and the manner in which data is processed across the Organisation.

Collection and use of personal information

The Organisation does not collect any personal data about you on this website, apart from information which you volunteer (for example by e-mailing the Organisation). Any information, which you provide in this way, is not made available to any third party - other than those working with the Organisation on normal Organisation business, and is used by the Organisation only in line with the purpose for which you provided it.

Collection and use of technical information

Cookies may be used by the INMO website to collect non-personal information about how visitors use our website or to remember display preferences. Temporary session cookies may also be used in some areas to enable specific functionality (e.g. portal pages). Session cookies are deleted once you close your browser session.

Occasionally for the purposes of INMO online services we must pass some cookie information to third parties. These cookies may persist after your browser session has ended. This information will not include any of your personal data or information from which you will be readily identifiable. This information may be used for evaluating your use of the website, compiling reports on website activity for INMO and providing other services relating to website activity and internet usage. It is stored and used in the aggregate only and is not used to obtain personal data or to contact you personally, but instead to improve website services. INMO actively seeks to preserve user privacy in any interaction with third parties.

Some areas within the INMO website use online data entry forms to collect personal information from web visitors who choose to identify themselves for the purpose of transacting e-commerce or receiving products, services, or information. Areas within INMO that collect data of any type are required to abide by our Data Protection Policy. We request no more information than is required to fulfil the purpose for which the information is being collected.

Technical details in connection with visits to this website may be logged by the Organisation's internet service provider for accounting and auditing purposes. This technical information will be used only for statistical and other administrative purposes. You should note that technical details, which the Organisation cannot associate with any identifiable individual, do not constitute `personal data' for the purposes of the GDPR and Data Protection Acts 1988 to 2018.

Personal Data Rights

You have a number of rights under personal data protection legislation. For further information on these please refer to our Data Subject Rights Procedure (APPENDIX H – Data Protection Policy).

For further information on personal data matters, including the contact details for the INMO Data Protection Officer, please refer to the Organisation's Data Protection webpage as referred to above.

APPENDIX M – WEBSITE COOKIES STATEMENT

Irish Nurses and Midwives Organisation
Website Cookies Statement

General statement

The Irish Nurses and Midwives Organisation fully respects your right to privacy, and will not collect any personal information about you on this website without your consent. Any personal information which you volunteer to the Organisation will be treated with the highest standards of security and confidentiality, in accordance with the GDPR and Data Protection Acts, 1988 & 2018.

Website Visits

When someone visits www.inmo.ie, or other websites maintained by the Organisation, we collect standard internet log information and details of visitor behaviour patterns. Some of the above information is used to create summary statistics, which allow us to assess the number of visitors to our site; identify what pages are visited most frequently and, ultimately, make the site more user friendly.

- We do not attempt to find out the identities of those visiting our website
- We will not associate any data gathered from this site with any personally identifying information from any source
- If we do intend to collect personal information we will make it clear and will explain what we intend to do with it

Certain pages on this site provide an option to request further information by email, or to provide feedback online. This information will only be recorded if you choose to send us a message and will only be used for the purpose for which you have provided it.

Use of Cookies

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

The majority of the cookies used on the INMO website, or other websites maintained by the Organisation, are associated with the use of Google Analytics. Google Analytics uses code, provided by Google, to collect information about how visitors use our site. The cookies collect information in an anonymous form that does not identify an individual. They provide information regarding the number of visitors to the site, where visitors have come to the site from and the pages they visited. We use this information to compile reports and to help us improve the way our website works, for example by making sure users are finding what they need easily.

The remaining cookies are INMO generated cookies and are used to customise the content provided to you. Should you decide to disable cookies at any time, some functionality of our website may be impaired.

APPENDIX N – DATA BREACH PROCEDURE

Irish Nurses and Midwives Organisation
Personal Data Breach Procedure

What is a Personal Data Breach?

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What to do?

1. Any staff member who is aware of or suspects a personal data breach must notify the Data Protection Officer (DPO) of the suspected data breach. In their absence advice should be sought from a member of the General Secretary or member of the Senior Management Team and references to the DPO should be read as referring to those persons where relevant.

2. The DPO will personally, or instruct others, to investigate the potential breach to establish if it is real. The Data Protection Officer will liaise with the General Secretary, or her designate throughout, and associated with, each step of this process.

3. The impact to individuals and organisations will be assessed.

4. The DPO will take all necessary immediate steps to secure all relevant personal data and to minimise the effects of the breach. Following consultation with the General Secretary, her designate, or a member of the Senior Management Team, the steps necessary to immediately secure data and minimise the effects of the breach may be coordinated by persons other than the DPO.

5. The DPO is responsible for notifying the Data Protection Commissioner (DPC) within 72 hours with details of:

    - The nature of the personal data breach
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the Data Protection Officer
    - A description of the likely consequences of the personal data breach
    - A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects

6. Note – it is only necessary to contact the DPC if the breach could result in:[3]

[3] The obligation on controllers to notify the competent supervisory authority arises in the case of any personal data breach, unless the breach is unlikely to result in "a risk" to the rights and freedoms of individuals.

- Discrimination
- Damage to reputation
- Financial loss
- Loss of confidentiality
- Economic disadvantage
- Social disadvantage

7. The DPO will notify any individuals concerned if there may be a risk to the rights and freedoms of those individuals. Following consultation with the General Secretary, her designate, or a member of the Senior Management Team, the steps necessary to notify data subjects may be undertaken by persons other than the DPO.

8. Resolve breach – to include the DPO/Others:

    - Undertaking a causal analysis;
    - Makin recommendations to prevent recurrences;
    - Relevant remedial measures undertaken and verified;
    - Written report of breach, decisions made and reasons for same, and a record of actions taken completed and retained by DPO.

The GDPR elaborates to a degree as to what might constitute a risk, noting in the recitals that where a breach is not addressed in an appropriate and timely manner, the risks can include a broad range of physical, material and immaterial damage, such as loss of control over personal data, financial loss, identity theft and damage to reputation.
Based on this broad understanding of risk, the notification obligation, with regard to the competent supervisory authority, will likely arise in a substantial number of breach events. However, even where no notifications arise, controllers should document the facts relating to the breach, its effects and any remedial action taken, in a manner that will enable the competent supervisory authority to verify compliance by the controller with its obligations to notify the competent supervisory authority in appropriate circumstances.

APPENDIX O – PROCEDURE WHEN PROVIDING MEMBERSHIP LISTS TO INMO REPRESENTATIVES

Irish Nurses and Midwives Organisation

Procedure for Provision of Membership Lists to INMO Representatives During Balloting/ For Membership Organisation Purposes

INMO representatives play a crucial role in the administration of the affairs the Organisation on an ongoing basis. They are a key aspect of our Organisational structure and their role is provided for under Rule. Their role in processing personal data held by the Organisation is comprehended by our Data Protection Policy, and this additional procedure provides guidance on the steps to be taken when providing membership listings to our representatives for balloting or membership organisation purposes.

1. Membership lists may be issued to INMO representatives, as provided for under Rule, and the identity or representatives can be ascertained by contacting the relevant Industrial Official;
2. The purposes for which lists may be issued are limited to – balloting and membership organisation purposes (e.g. mapping);
3. On any occasion where a membership list is issued the attached notice must accompany the issuing of the membership listing;
4. A record must also be kept by the person issuing the list as to who it was issued to, the date it was issued, and the time period for return of the list;
5. A record must be maintained as to whether the list was returned, and if not contact must be made by the person who issued the list with the representative to secure its return, or alternatively to agree a revised return date. Thereafter, if not returned the matter must be discussed with the relevant Industrial Official who will take other necessary steps to secure the return of the list, or alternatively engage the Personal Data Breach Procedure.
6. Questions in relation to this procedure can be addressed to the relevant Industrial Official or the Data Protection Officer.

Notice to INMO Representatives
Important Information – Data Protection & INMO Membership List

As a representative of our Organisation you are provided with a membership list to allow you undertake varying functions, including, mapping of our membership, and the conducting of ballots. However, in providing you with this information, we are providing you with sensitive information (personal data) in relation to our members, and we are very anxious to ensure that we both comply with the law in relation to data protection, and effectively protect the interests of our members.

It is legitimate to share this information with you so that you can carry out functions related to our relationship with our members, and the activities of the Organisation. It is also legitimate as you are a representative of this Organisation, and therefore have a key function to undertake in accordance with our Rule book.

That said, all persons who are associated with the Organisation, including staff, representatives, and those appointed to assist with specific tasks, have duties, roles and functions which touch upon the rights and interests of our members in relation to their personal data. A full description of the duties, roles, functions and principles associated with Data Protection and the activities of the INMO is available in our Data Protection Policy which is available at www.inmo.ie/dataprotection.

Therefore, in receiving this list we ask you to take care in relation to the following;

1. Please note that this list does contain personal data in relation to our members, which is of a sensitive nature. Therefore, it must be treated with care, must be maintained absolutely confidential, and must be stored securely.
2. Additionally, the information must only be used in accordance with the purpose for which the list was given to you. For example, if the list is provided for balloting purposes, the information must only be used for checking the membership of a person in respect of casting their ballot. If the list is provided to you for mapping our membership, it must only be used for that purpose, and no other purpose.
3. If the list has been shared with you for the purposes of balloting, and you are sharing the list with any other representative, or person appointed by the Organisation to assist with balloting, it is essential that you provide them with this information sheet to ensure that they understand their responsibilities in relation to the information.
4. Once you have concluded the purpose for which the information has been provided to you, it is necessary that you return this membership listing to our Organisation. For example, if you are conducting a ballot, the list must be returned at the conclusion of the ballot. If you are carrying out membership mapping, we ask that you retain the information securely and confidentially, for a maximum period of three months and then return it to the Organisation, if your mapping concludes earlier please return the list as soon as the task is completed.

The role you undertake with the Organisation is essential, and you are an essential part of our Organisation. All of us wish to ensure that the information shared with us by our members is used only for purposes which are legitimate, that we maintain that information in a secure and confidential manner, and that in all aspects we comply with relevant data protection law. We appreciate your ongoing efforts on behalf of the Organisation, and in addition, your strict compliance with the information contained in this notice.

If you have any concerns or queries, or any issues arise from us providing you with this list, please contact your Industrial Official immediately.

APPENDIX P – SERVICE/COMMS ROOM POLICY

IT Server/Comms Room
One Server/Comms room which is located in the basement of INMO HQ, The Whitworth Building, North Brunswick Street, Dublin 7 D07 NP8H

1. Purpose

The purpose of this policy is to ensure a minimum level of security is maintained by all staff that have access to the IT Server/Comms Room and in compliance of our Data Protection Policy.

2. Scope

The following policy is currently applicable to staff that have access to the IT Server/Comms Room based in Irish Nurses and Midwives Organisation, The Whitworth Building, North Brunswick Street, Dublin 7 D07 NP8H and all visitors requiring access to the IT Server/Comms Room.

3. Roles and Responsibilities

3.1 **IT Manager:** It is the responsibility of the IT Manager and IT Senior Systems Manager to ensure that this policy is enforced and complied with. The IT Manager is responsible for holding and maintaining any Access Log or record of entry/exit.
3.2 **All other staff with rights to access:** All staff must be aware of this policy and their obligations therein. It is their responsibility to ensure they carry out their duties in a professional manner whilst working in the IT Server/Comms Room.
3.3 **Visitors:** All visitors requesting access need to be made aware of this policy and their obligations therein. It is the responsibility of the member of IT dept. accompanying the visitor to ensure they carry out their duties in a professional manner whilst working in the IT Server/Comms Room.

4. Access to the IT Server/Comms Room

- Physical access to the server room must be limited to only those individuals who have legitimate responsibilities justifying such access. Procedures will be in place to ensure access is removed when an individual no longer has such need.
- A current list of Server/Comms Room Access is listed in Appendix A Below.
- The primary mechanism for controlling access to the IT Server/Comms Room is via a standard bolt door lock. There is also protection via the fire detection system.
- All authorised staff are required to be signed in and out of the IT Server/Comms Room Access Log. These log sheets are retained by the IT Manager/ IT Assistant. All visitors must also be recorded in the IT Server/Comms Room Access Log.
- Visitors access must be supervised and facilitated by IT Department staff.
- Unauthorised access into the IT Server/Comms Room must be reported, in addition to informing the IT Manager of the breach of security.
- Entry into the IT Server/Comms Room by tailgating other staff is not permitted.

- Physical audits of the server room will be periodically undertaken by IT Department given that 3rd parties have access. This negates increases risk to IT Infrastructure given these 3rd party users, such as phone company access the Comms room.
- Working to limit physical access to the server room is an important part of an IT security plan. Controlling access can help protect against both intentional and unintentional events that may damage the computing environment and result in significant productivity and revenue losses.
- The use of mobile phones, pagers or other equipment that emits radio waves within the IT Server Rooms is forbidden unless specific exemption is obtained from the IT Manager.
- Food and drink must not be taken into the IT Server/Comms Room.
- Monthly the IT Manager will review the Access Log; the Log will be signed at the last entry and dated.

A procedure for the safe use of the room facilities within the IT Server/Comms Room will be made available from the Facilities Manager. This will mainly be concerned with the safe use of the fire safety system in the room.

5. Training and Awareness

All relevant staff will have this policy brought to their attention by the IT Manager. The policy will also be available via the IT Manager. Any queries regarding this document will be dealt with by the IT Manager.

6. Review

This policy will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

7. Discipline

Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the INMO's Disciplinary Procedure.

8. Emergency Key

A security box on wall outside Comms Room with have a key which will be accessible via a code given in the case of an emergency.

Appendix A -IT Server/Comms Room Access List

Current Key Holders

- Muriel Haire – IT Manager
- David Cummins – IT Assistant
- Stuart McNeill/Wayne McNeill

Lost or stolen keys must be reported immediately to the IT Manager.

APPENDIX Q – POLICY FOR SECURE USE OF USB MEMORY DEVICES

Policy Purpose

The policy provides guidance to staff on the secure use of USB memory sticks for carrying confidential, sensitive and Person Identifiable Data (PID) (service users & staff). This policy is in accordance with our Data Protection Policy

Scope

USB memory sticks have become increasingly popular because of their small physical size and large storage capacity. This has made them very convenient devices for carrying files from one place to another.

However, these very features have introduced new information security risks:

- Loss of information – a memory stick, like a computer, is susceptible to data loss or failure.
- Potential breach of confidentiality – if the memory stick is lost or stolen.
- Physical loss – being so physically small the memory stick can be easily lost.
- Corruption of data - if the memory stick is not removed from a computer properly.
- Virus transmission – memory sticks can introduce viruses onto a computer network.

Staff Responsibility

There are two main ways of preventing the loss of information:

- Staff members should not use any USB key in any INMO computer which has not been provided to them by the IT Department
- Staff should avoid physically carrying INMO information on USB Keys
- Staff must request from the IT department and encrypted USB Key should case arise for confidential, sensitive & Person Identifiable Data to be stored on a USB Key.
- Staff should use other secure methods for carrying such information: Either by storing information on local personal H Drive or by storing information in departmental folders on the shared 'I' drive. Your departments 'I' drive folder can be access on any INMO networked computer. For Home Office users it is recommended that you store all your data on your laptop hard drive and not on USB keys or external devices.
- USB Keys given to staff must be returned to IT Department when no longer required, if keys are not returned, the USB Key is the responsibility of each staff member to keep the key in a safe place and remove data when it is no longer been used from the USB key.

Encryption / Safety of Sensitive Data

- Where a need has been identified and agreed with IT Department an encrypted memory stick is required to carry confidential, sensitive or PID, a request must be made via the IT Department for an INMO IT Service approved encrypted device.

- An encrypted memory stick allows information to be stored but renders the information undecipherable unless the correct password is entered. Encrypted memory sticks will be issued to specifically named members of staff for their professional use. Staff Members must not share the device with other persons. They must not share or disclose the password to other persons.
- **NB** Confidential, sensitive or PID (personally identifiable data) carried on encrypted memory sticks must not under any circumstance be placed on non INMO issued computers.
- Such information must always remain on the encrypted device and be immediately transferred onto users departmental 'I' or 'H' drive files and deleted from the encrypted memory stick once no longer required to be on the device.
- A register will be maintained by the IT Department of all encrypted memory sticks issued. All issued encrypted memory sticks remain the property of INMO and must be returned when staff leave employment with INMO or no longer need to use such a device.
- All staff have a duty of care to ensure all confidential, sensitive and PID is always held securely. The loss of confidential, sensitive and PID information is extremely serious and if a member of staff is found to be using a non-encrypted memory stick for carrying confidential, sensitive and PID information they may be subject to disciplinary procedures.
- Staff are currently permitted to use non-encrypted USB memory sticks for carrying non-confidential and non-sensitive information although this position will be regularly reviewed. All losses of confidential, sensitive and PID must be reported on the IT Department immediately.
- "Where in exceptional circumstances, use of an external storage device could be implemented when all reasonable alternatives have been exhausted" (i.e- no access to internet/Wi-Fi, loss of primary secured device/data etc).

Training and Awareness

All relevant staff will have this policy brought to their attention by the IT Manager. The policy will also be available via the IT Manager. Any queries regarding this document will be dealt with by the IT Manager.

Review

This policy will be reviewed in accordance with the frequency of review of the main Data Protection Policy. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

APPENDIX R – POLICY FOR INTERNAL MANAGEMENT OF DATA ACCESS REQUESTS

1. Policy Purpose

The policy provides guidance to the DPO and administrative staff working with the DPO in responding to data access requests. It also provides guidance to staff facilitating the DPO in responding data access requests.

2. Scope

This policy applies to the DPO, administrative assisting the DPO, and all staff assisting the DPO in responding to a data access request in furtherance of the statutory rights of a data subject.

3. Staff Responsibility

Data Protection Officer (DPO): The DPO is responsible for responding to and managing data access requests in accordance with the statutory rights of data subjects, including the management of requests with reference to the rights of third parties, and the position and policies of the Organisation bearing in mind the applicable statutory provisions. Administrative staff working directly with the DPO will work under the direction of the DPO and are responsible for carrying out the directions of the DPO and for adhering to this policy, and the Data Protection Policy overall.

All Staff: All staff who are directed by the DPO are responsible for responding to the requests made by the DPO in a timely fashion bearing in mind the statutory timeframes applicable to responding to data access requests. Those staff are also responsible for adhering to this policy, and the Data Protection Policy overall.

4. Management of Data Access Requests

1. Upon receipt of a data access request the DPO will acknowledge the request.
2. The DPO will set in motion of process to gather potentially relevant data in furtherance of a data access request.
3. Any staff member requested to provide personal data in relation to a data subject which may be under their control, or accessible by them, will – in accordance with the terms of the request:
    - Conduct a search of relevant paper files, to include case files and other relevant notes, and provide a full original copy of all paper containing personal data held to the DPO. Staff should be conscious that in some instances this may necessitate access to more than one paper file/source. Staff should also be conscious that where personal data relating to the data subject to whom the request relates is contained in a mixed file, e.g. one dealing with a particular service, the full paper file should be provided to the DPO, with the relevant papers referring to the data subject tagged, so that an appropriate analysis of the data access request can be carried out.

- Conduct a search of our central database and provide a reproduced paper copy of any personal data contained in the central database which is not already contained in the paper file referred to above.
- Conduct a search of our membership system and associated records, and provide a reproduced paper copy of any personal data contained in that database, to include all entries which constitute personal data, which are not already contained in the paper file referred to above.
- Conduct a search of their email systems/database, including where relevant the email systems of administrative assistants, and provide a reproduced paper copy of any personal data contained in that database, to include all entries which constitute personal data, which are not already contained in the paper file referred to above.
- When searching for email records containing personal data, please ensure that the data reproduced, and which refers to the data subject, includes emails sent and received.
- All these materials must be conveyed to the DPO without delay, bearing in mind that save in exceptional circumstances data access requests must be addressed within one month.
- Staff in turn, where further clarification or requests are received/made by the DPO will respond in a timely fashion.

4. The received data will be analysed by the DPO to establish which data comes within the parameters of the request, and to ensure that the rights of other data subjects are respected.
5. The DPO will prepare the data which is to be released, pursuant to the data access request and provide same to an administrative employee to prepare the data for conveyance to the data subject. Two copies will be prepared, one for conveyance and one for INMO records.
6. Once prepared for conveyance to the data subject a further review will be carried out by the DPO prior to the data being forwarded to the data subject, pursuant to the data access request.
7. If approved upon second review – the data reviewed, without alteration, will be conveyed to the data subject and the copy stored in a data access request file. However, if alterations are required then step 6 will be repeated prior to release.

5. Training and Awareness

All staff will have this policy brought to their attention by their Line Manager. Any queries regarding this document will be dealt with by the Line Manager in the first instance, and further assistance can be obtained from the DPO.

6. Review

This policy will be reviewed in accordance with the frequency of review of the main Data Protection Policy. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

APPENDIX S – STAFF DATA PROCESSING NOTICE:

1. Introduction

This Notice describes the practices of the Irish Nurses and Midwives Organisation ("the Organisation/INMO") regarding the collection, use, transfer, disclosure and other handling and Processing of your Personal Data as an employee of INMO.

In particular, the INMO is committed to Processing the Personal Data of its employees in a fair, lawful and transparent manner. Accordingly, this Notice provides INMO employees with certain information about how their Personal Data is used by INMO. INMO has also adopted a Data Protection Policy (the "Data Protection Policy INMO") that addresses data protection more generally. Capitalised terms used in this Notice are defined in the Glossary in Appendix I to this Notice.

In relation to Personal Data provided by you to INMO, INMO will act as Data Controller of such Personal Data. This means that INMO determines why and how such data is used, within the confines of applicable legal rules.

2. What is Personal Data?

Personal data is any information relating to a living individual which allows either directly or indirectly the identification of that individual. Personal Data can include a name, an identification number, details about an individual's location or any other detail(s) that is specific to that individual and that would allow the individual to be identified or identifiable.

The type of Personal Data that INMO collects and Processes in relation to employees is described in more detail in the table at Appendix II of this Notice.

3. How we Collect and Use your Personal Data

The table at Appendix II also describes in detail the particular purposes and lawful basis for INMO's Processing of employee Personal Data as required by Data Protection Law. INMO will generally Process your Personal Data for personnel administration purposes and for purposes necessary for and connected with the performance of its objects and functions as an employer and related legislation.

INMO may obtain Personal Data about you from third parties, such as former employers, educational institutions, recruitment agencies, recruitment platforms such as LinkedIn, government agencies, from information in the public domain and available on the internet and from other employees (e.g., other INMO staff, supervisors, members of the HR Department, etc.).

We may also seek Personal Data about you from third parties in connection with: (I) locating former employees and beneficiaries for purposes of administering retirement, pension or other benefits; (II) performance evaluations; (III) academic and processional references; (IV) disciplinary matters and internal investigations; (V) purposes that relate to your employment relationship with us; and (VI) other purposes permitted in accordance with applicable law. Where we obtain Personal Data about you from third parties, we will do so in accordance with Data Protection Law.

4. Special Categories of Data

INMO Processes Special Categories of Data ("SCD") relating to employees in limited circumstances, typically related to the ordinary course of personnel administration which is in accordance with the Data Protection Law.[4] Such Processing of SCD is permitted under several provisions of the Data Protection Law, including the following:

1. Article 9(2)(f) GDPR where it is "necessary for the establishment, exercise or defence of legal claims" and this ground is amplified in [Section 41 of the Data Protection Act 2018] which permits the Processing of SCD where it is necessary for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights (and which may include Processing in the context of disciplinary proceedings);

2. Article 9(1)(g) GDPR which permits such Processing for reasons of substantial public interests and this is amplified in [Section 43 of the Data Protection Act 2018] which provides a general lawful basis for Processing of SCD where it is necessary and proportionate for the performance of a function conferred by or under an enactment; and

3. In relation to the management of medical risk and medical claims, [Section 46 and 47 of the Data Protection Act 2018] permit the Processing of SCD where it is necessary for the purposes of preventative or occupational medicine, to assess the working capacity of an employee, for the management of health or social care systems and services or for ensuring high standards of quality and safety of health care.

5. Your rights under Data Protection Law

Data Protection Laws provide certain rights in favour of data subjects.

The rights in question are as follows (together the "Data Subject Rights"):

a) the right of a data subject to receive detailed information on the Processing (by virtue of the transparency obligations on the Data Controller);
b) the right of access to Personal Data;
c) the right to rectify or erase Personal Data (known as the "right to be forgotten");
d) the right to restrict Processing;
e) the right of data portability;
f) the right of objection (in circumstances where Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller); and
g) the right to object to automated decision making, including profiling.

Please note that Articles 17 and 20 GDPR state that the right to be forgotten and the right of data portability do not apply to Processing that is necessary for the performance of a task

[4] Comment: Section 40 of the Data Protection Act 2018 provides a general lawful basis for Processing SCD where it is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the controller or the data subject in connection with employment or social welfare law. As required by Data Protection Law INMO applies suitable and specific measures in respect of such Processing.

carried out in the public interest or in the exercise of official authority vested in the Data Controller. Accordingly, these rights and the other Data Subject Rights may not be available to you in certain circumstances.

Any data subject wishing to exercise their Data Subject Rights should contact the INMO Data Protection Officer ("INMO DPO"). Your request will be dealt with in accordance with INMO's Data Subject Rights Procedure. For further information on your Data Subject Rights please refer to the above document.

6. Data Security and Data Breach

We have technical and organisational measures in place to protect Personal Data from unlawful or unauthorised destruction, loss, change, disclosure, acquisition or access. Personal Data are held securely using a range of security measures including, as appropriate, physical measures such as locked filing cabinets, IT measures such as encryption, and restricted access through approvals and passwords.

The GDPR obliges Data Controllers to notify the Data Protection Commissioner and affected data subjects in the case of certain types of Personal Data security breaches (Art. 34). We will manage a Data Breach in accordance with our Data Breach Reporting Procedure. For further information on identifying and reporting a Data Breach please refer to the above document. If you become aware of, or suspect that a Data Breach has taken place, you are required to immediately notify the INMO DPO by both phone and email.

7. Disclosing Personal Data

From time to time, we may disclose Personal Data to third parties, or allow third parties to access Personal Data which we Process (for example where a law enforcement agency or regulatory authority submits a valid request for access to Personal Data).

We may also share Personal Data: (a) with another statutory body where there is a lawful basis to do so; (b) with selected third parties including sub-contractors; (c) if we are under a legal obligation to disclose Personal Data. For example, this may include where a member of staff spends time in another institution or is seconded to/from a government department or body and also includes exchanging information with other organisations for the purposes of fraud prevention or investigation.

Where we enter into agreements with third parties to Processes Personal Data on our behalf, we will ensure that the appropriate contractual protections are in place to safeguard such Personal Data where required by Data Protection Law. Examples of such third party service providers that we engage, and to whom we may provide Personal Data include but are not limited to communications providers, payroll service providers, pension administrators, occupational health providers, marketing or recruitment agencies, operators of data centres used by us, security services, catering service providers, and professional advisors such as external lawyers, accountants, tax and pensions advisors.

8. Data Retention

We will keep Personal Data only for as long as the retention of such Personal Data is deemed necessary for the purposes for which the Personal Data are Processed. Further details of the retention period for Personal Data is set out in our Data Retention Policy.

9. Data Transfers outside the EEA

Although unlikely, we may need to transfer Personal Data outside the EEA. If necessary, this transfer will occur in accordance with applicable Data Protection Law. We take reasonable steps to ensure that the Personal Data is treated securely and in accordance with the INMO Data Protection Policy when transferred outside the EEA.

10. Further Information/Complaints Procedure

You can ask a question or make a complaint about this Notice, the INMO Data Protection Policy and/or the Processing of your Personal Data by contacting the INMO DPO. While you may make a complaint in respect of our compliance with Data Protection Law to the Irish Data Protection Commission, we request that you contact the INMO DPO in the first instance to give us the opportunity to address any concerns that you may have.

Glossary

In this Notice, the terms below have the following meaning:

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

"Data Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the party that Processes Personal Data on behalf of the Data Controller (for example, a payroll service provider).

"Data Protection Law" means the General Data Protection Regulation (No 2016/679) ("GDPR") and the [Data Protection Act 2018] and any other laws which apply to INMO in relation to the Processing of Personal Data.

"European Economic Area" or "EEA" means Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK, Iceland, Liechtenstein, and Norway.

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Process" and "Processing" are interpreted accordingly.

"Special Categories of Personal Data" (or "SCD") are types of Personal Data that reveal any of the following information relating to an individual: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Special Categories of Personal Data also include the Processing of genetic data, biometric data (for example, fingerprints or facial images), health data, data concerning sex life or sexual orientation and any Personal Data relating to criminal convictions or offences.

Data Processing Purposes

The following table describes the type of Personal Data that is collected by the INMO relating to INMO employees and the purposes and lawful basis for Processing that data under by Data Protection Law:

Description of Personal Data	Purpose of Processing	GDPR lawful basis
Information contained in: CVs, cover letters and job applications (including previous employment background, education history, professional qualifications, references, language and other relevant skills, certification, certification expiration dates), interview notes and feedback; details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate or driver's license information.)	Recruitment, personnel administration and HR management, including performance analysis and promotion purposes.	Contract performance (Art 6(1)(b)).
HR files and records (including CPD and training records, disciplinary records, salary details, benefits, compensation type, pay grade, salary step within assigned grade, awards, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data, national insurance or other number, marital/civil partnership status, domestic partners and dependents).	Personnel administration and HR management, including performance analysis and promotion purposes.	Compliance with legal obligations under employment legislation (Art 6(1)(c); and Contract performance (Art 6(1)(b)); and Protecting the vital interests of employees and other persons (Art 6(1)(d)).
Photographs of employees	For use in INMO publications and website so members can identify Officers and staff of the Organisation, and to publicise the activities of the Organisation to its members; For use on Outlook to enable staff to identify colleagues.	Contract performance (Art 6(1)(b)); and Protecting the vital interests of employees and other persons (Art 6(1)(d)).

Data related to pensions	To enable INMO pension trustees and related service providers to administer your pension entitlements.	Contract performance (Art 6(1)(b)).
Medical information (including medical certificates and sick notes).	Personnel administration and to verify employee absences from work on sick leave and purposes of preventative or occupational medicine.	To assess the working capacity of an employee (section 46 Data Protection Act 2018).
Name, role, email address (work), telephone number (work), office number, profile photograph and details of: previous roles, research areas/interests and academic publications.	For publication on various sections of INMO website and in hard copy materials.	Contract performance (Art 6(1)(b)).
Data Processed in relation to optional staff schemes or benefits	In relation to Travelpass, Bike-to-work scheme etc.	Employee consent, which can be withdrawn at any time (Art 6(1)(a)); and Contract performance (Art 6(1)(b)).
CCTV Footage	The INMO has closed circuit television cameras ("CCTV") located in its various offices covering buildings, some internal spaces, car parks, roads, pathways and grounds. The INMO's CCTV system is implemented in a proportionate manner as necessary to protect INMO property against theft, pilferage or damage, and for the safety and security of staff, members and visitors to our facilities (to protect their vital interests). CCTV footage may only be monitored on the permission of the General Secretary, or her designate, and access to recorded footage is strictly limited to authorised personnel. Requests to access, and authorisation provided, will be recorded in writing and retained by the Data Protection Officer.	Protecting the vital interests of employees and other persons (Art 6(1)(d)).

	Footage is retained for 28 days, except where incidents or accidents have been identified in which case such footage is retained specifically in the context of an investigation of that issue. CCTV footage may be used in the context of disciplinary proceedings involving INMO staff or members (to protect the vital interests of the INMO, staff, members and affected individuals). CCTV footage is not disclosed to third parties except where disclosure is required by law (such as for the purpose of preventing, detecting or investigating alleged offences) and in such instances disclosure is based on a valid request.	
Name, contact details of employees, and all other visitors to INMO offices Personal Data related to health, as recommended by national health authorities and the Government for the purposes of managing business operations in the context of Covid-19.	Allow continuation of business activities in the context of Covid-19, and to manage activities to assist in controlling the spread of the virus as recommended by national health authorities and the Government.	Protecting the vital interests of employees and other persons (Art 6(1)(d)); Necessary for the purposes of the legitimate interests pursued by INMO under Art. 6(1)(f); and Necessary for a task carried out in the public interest (Art. 6(1)(e).

APPENDIX T – CARD PAYMENT POLICIES AND PROCEDURES

1. Introduction & Purpose

This policy and procedures document has been created to assist employees of the INMO (the Organisation) in understanding the importance of protecting credit/debit cardholder data and to inform employees on the rules surrounding safeguarding this information.
All staff members who have roles which require access to cardholder data, or roles which make it possible to obtain access to cardholder data, have a responsibility to protect that data. This document lays out a set of requirements to which all staff of the Organisation who access to cardholder data must adhere. This policy will apply to staff who are authorised to process credit/debit card payments, and only staff authorised by the General Secretary or Deputy General Secretary may process such payments.
The ability to facilitate payments by members over the phone, or by use of payment terminal, is important to assist the Organisation in providing services to members and to provide an efficient and secure means for members to pay for certain services or events.
However, it is also important that we comply with industry standards in relation to expected policies, procedure, and practice. Additionally, it is essential that we safeguard the information provided to us and the interests of those we deal with as a matter of law, best practice, and in the interests of the Organisation and its reputation. As an organisation which processes cardholder data, this includes an obligation to comply with the Payment Card Industry Data Security Standard (PCI-DSS).

2. What is PCI-DSS? (Payment Card Industry Data Security Standards)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards introduced by VISA, Mastercard and other payment brands that applies across the card payment industry worldwide. It helps safeguard cardholder information, improve customer confidence, and reduce the risk of fraudulent transactions. These rules are compulsory for all organisations handling any aspect of card transactions who have access to cardholder data.

There are 12 requirements to PCI-DSS, these include:

Control Objectives	**Requirements**
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software

	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

Card Payment Data
Card payment data consists of 2 main sets of data that must be protected by the Organisation at all times. These include:

Cardholder Data	**Sensitive Authentication Data (SAD)**
Primary Account Number (PAN) i.e., the 16-digit number on the front of the card	Full Magnetic Stripe Data/Chip Data
Cardholder Name	CAV2/CVC2/CVV2/CID i.e., the last 3 digits on the signature strip on the back of the card
Expiration Date	Pin Numbers
Service Code	

PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. In the course of taking payments, we may process the PAN and as such the requirements apply to the Organisation.

3. Purposes of the Policy and Procedures

These procedures deal with the acceptable use and the controls required for receiving, processing and storing information in respect to all card data and covers all electronic and manual handling methods, including:

Card Present Transactions	**Card Not Present Transactions**
Face to Face (Chip and pin)	Internet
Face to Face Contactless	Telephone

These procedures cover the security of cardholder data and must be distributed to any staff of the Organisation who process credit/debit card transactions. The procedures shall be reviewed

annually and updated as needed to reflect changes to business objectives, to the risk environment or to PCI-DSS.

4. Acceptable Use

The processing of card data potentially gives rise to data protection concerns, and as a result the Data Protection Policy of the Organisation contains important information, which is also included in this document.
The processing of card data is legally permissible only for the purposes for which the data was provided, i.e., the transaction in question. Any other, or subsequent, use of the card data for an unauthorised purpose is in breach of data protection principles and law, may give rise to criminal prosecution, and in addition would amount to serious or gross misconduct within the meaning of the disciplinary procedures of the Organisation. The card data provided for the purposes of a specified transaction may only be used for that transaction, may not be stored by the Organisation in any form whatsoever, and must not be disclosed to any other person within or outside the Organisation. A failure to comply with the policy set forth in this document, and the associated procedures, may result in disciplinary action up to and including the termination of employment.

To ensure compliance, the key areas that need to be addressed and implemented by staff who undertake card transactions are:

- Access to payment card transactions and data must be restricted to only those members of staff who need access as part of their role.
    - Only staff authorised by the General Secretary or Deputy General Secretary may process card transactions.
    - This authorisation will be communicated in writing or by email to the relevant line manager and to the Accounts Department Manager who will maintain a list of authorised persons.
- Staff should be aware of the importance and confidentiality of card payment data and under no circumstances should credit card numbers be stored or transmitted in paper form, or electronically, this includes e-mailing, instant messaging, chat or any other medium.
    - All staff who are authorised to process card transactions will be provided with training in relation to the use of the relevant technology.
    - All staff who are authorised to process card transactions must first read this policy, and prior to being involved in the processing of card transactions must indicate in writing or by email that they have read and understood this policy and its associated procedures. This confirmation must be sent to the Accounts Department Manager who will maintain a record of these confirmations.
    - Card payment data **MUST NOT** be written down. This includes when taking payments over the phone. If for some reason the payment cannot be input immediately the caller's contact details should be taken and a call-back arranged.

- If taking payments over the phone care must also be taken to ensure that you do not call out the details, or read back the details to the caller, in a place or manner which would allow these details to be overheard by others.

- If card details are sent to you by unauthorised means, e.g., in an email or via the post, please immediately delete the email, or securely destroy the paper copy, and then contact the person to inform them that this has occurred. Explain that you cannot process the details sent to you in the interests of security, and as a result you can then offer them an alternative route e.g., by taking a payment over the phone.

- If using a terminal to process an in person transaction you must ensure that the person enters their PIN in a manner whereby you cannot see the PIN being entered.

- It is strictly prohibited to send, receive, process and store card details by Unapproved Methods.

Please Remember

Card payment data MUST NOT be written down. This includes when taking payments over the phone.
If for some reason the payment cannot be inputted immediately the caller's contact details should be taken and a call-back arranged.

5. INMO Approved Card Payment Methods and Services

Card Holder Not Present

Online Payment via INMO Approved Solution

- This arises where for example a member pays their membership fee via the INMO website.
- Mandatory Controls:
  - Payment via online system should generate an e-mail payment confirmation to the customer.
  - If a person's payment has been unsuccessful or declined, the person should contact their card provider in the first instance.
  - If a person faces difficulty in making a payment, then staff assistance can be provided.
  - If the payment problem cannot be resolved, the person should be offered an alternative payment method.
- Storage of Card Data:
  - No.
  - Data is held by the approved INMO PCI-DSS compliant supplier.

Telephone Payment

- This will arise in the context of membership payments, payment for professional courses, and payment for other events.
- Mandatory Controls:

    - Where card details are provided during a telephone call, these must be processed directly into the PDQ terminal at that time. The card details must not be written down.
    - When card details are being provided during a telephone call, these must not be repeated back to the customer in such a way that it can be intercepted by third parties.
    - If it is not possible to process the card details directly into the PDQ terminal immediately then a call back must be offered.
- Storage of Card Data:
    - No.
    - Data is held by the approved INMO PCI-DSS compliant supplier.

Card Holder Present

Face-to-face Transaction Including Contactless

- This would arise in circumstances where we provide a physical terminal to facilitate care transactions.
- Mandatory Controls:
    - For contactless payments ensure the person checks the value of the transaction before swiping their contactless card or device over the terminal.
    - When the customer is present the card should be processed through the terminal according to the on-screen instructions. Only the person should handle their card unless you must check a signature.
    - If the transaction is successfully processed, the merchant copy should be securely stored and the customer copy given to the person.
    - If the transaction is declined, the person should be advised immediately, politely and in a discrete manner.
    - The customer copy stating that the payment was declined should be given to the person and the merchant copy should be stored securely.
    - The option of paying with a different card should be offered.
- Storage of Card Data:
    - Only merchant receipts are held in secure physical storage, and the person's card number is truncated, and disposed of as confidential waste.
    - Merchant receipts are stored confidentially by the Accounts Department and destroyed securely when no longer required. If a terminal is used outside of the Organisation's premises, then the receipts are stored securely by the staff member using the terminal and returned to the Accounts Department at the earliest opportunity.

Approved Online Systems and Terminals

The Organisation provides online systems and card payment processing terminals which are approved and PCI-DSS compliant.

The online systems ensure that the relevant card payment data is securely processed and stored via approved payment service providers. The approved provider and the system are PCI-DSS compliant and should be used for all such payments. The online system available to members to pay their membership fee is one system, and the other system is an online portal to facilitate the take of telephone payments.

The terminals in use have been selected to ensure that appropriate controls are in place to minimise risk, for example, the card number which appears on both the customer and merchant copies of receipts are truncated.

Only the General Secretary, or Deputy General Secretary, in accordance with the standard financial control procedures applicable to the Organisation can authorise a change in service provider.

6. Unapproved Card Payment Methods

Receiving information in relation to card payments via the following methods is not approved:

- Post/Written
- Email
- Fax
- Instant or social media messaging
- Voicemails/Recordings
-

Accepting cardholder data via the above methods exposes the Organisation to non-compliance with the PCI-DSS. This may result in fines, reputational risk if there is a data breach and ultimately potential withdrawal of the facility to take payments by credit and debit cards.

If card details are sent to you by unauthorised means, please immediately delete the material securely, and then contact the person to inform them that this has occurred. Explain that you cannot process the details sent to you in the interests of security, and as a result you can then offer them an alternative route e.g., by taking a payment over the phone.

Please Remember

Under no circumstances should the non-approved payment methods be used.

7. Storage of Card Payment Data

Firstly, the storage of any card payment data is not permitted without the authorisation of the General Secretary, Deputy General Secretary or if unavailable another member of the Senior Management Team.

Limited and exceptional circumstances may arise where data may need to be stored, e.g., for regulative, legislative, or operational reasons. In cases where this arises, and storage has been authorised, then ONLY the data below can be stored:

- Truncated card number – First 6 or last 4 digits only
- Cardholder Name
- Service Code
- Expiration Date
-

Where such data must be stored for the specified reason, and with prior authorisation, then it must be stored securely by the Accounts Department or by the relevant member of the Senior Management Team as appropriate.

Under no circumstances should such data be stored in any information technology system, nor can it be transmitted by email. Should it become necessary to transmit the information for regulative, legislative, or operational reasons then this must only be undertaken in paper form with appropriate security arrangements in place.

8. Third Party Approved Suppliers

Any third party appointed to manage cardholder data on behalf of the Organisation must be an approved and trusted supplier.

The third party must be audited on an annual basis and PCI-DSS certification must be evidenced.

The Accounts Department Manager will maintain a central list of service providers who store, process, or transmit cardholder data.

9. Security Management and Incident Response Plan

The areas which credit card data is processed or held is referred to as the Card Data Environment (CDE).

General Security Responsibilities:

- All users within the CDE must familiarise themselves and follow the policies and procedures applicable to their area of responsibility.
- All users within the CDE must only carry out their designated role.
- All users must not disclose their passwords or share accounts.
- All users within the CDE must take appropriate steps to secure devices and data from unauthorised access and protect them from damage.
- Only INMO supplied equipment should be used in connection to card processing, no personal devices should be used or connected to the systems.
- Users must not install, copy, or modify any software or devices in the CDE without authorisation.
- Computers, devices, and technologies used for card processing should only be used for official INMO business.
- All users must immediately report security incidents to their line-manager who will co-ordinate with relevant teams within the university.

The Organisation employs best practice guidelines, and engages trusted third part IT companies, to provide ongoing guidance and services to maintain the integrity and security of our devices and systems. All users must comply with general and specific requirements and directions which are in place, and which will change from time to time, to maintain the security and integrity of our devices and systems.

An incident may arise where there has been a deviation from this policy and associated procedures, or a security breach, or other matter of concern which touches on the integrity of the card payment system, the security of data, the potential misuse of data, or suspected actions which may reflect on the integrity and reputation of the Organisation.

Where such an incident is detected the person who becomes aware of the issue should immediately inform the General Secretary or Deputy General Secretary, or in their absence a member of the Senior Management team. They should also inform the Accounts Department Manager or her designate.

In response to any incident – the General Secretary or Deputy General Secretary, or in their absence a member of the Senior Management team, will manage, in an overall sense, the response to the incident. The Accounts Department Manager, or her designate, will be centrally involved in the coordination of the response. In addition, and as necessary, the assistance of external experts will be commissioned to assist with the response.

In the event of a breach or security incident the Organisation will take prompt action and follow an approved incident plan, the plan includes steps in line with recommended best practice to:

1. Preserve evidence.
2. Provide an initial investigation report and inform acquirer.
3. Procure approved external forensic capability if needed.
4. Assess all exposed accounts.
5. Provide a final investigation report.

10. Review

This policy and associated procedures will be reviewed annually.

APPENDIX U – USE OF INSTANT MESSAGING

Policy Purpose

The purpose of this policy to ensure protection of personal data of partners of the Organisation, and to ensure the appropriate and effective use of instant messaging platforms.

Scope

This policy is applicable to all partners of the Organisation in the meaning of section 4.2 of the main data protection policy, which includes staff, contractors, Executive Council members, INMO representatives, and ordinary members.

Requirements

- Any instant messaging group, e.g. WhatsApp groups, established by a staff member of the INMO must be limited in scope and function to:
    - Scheduling meetings.
    - Notification of members of the group to consult their emails for further information on a given topic.
    - Changes to scheduled meetings or events.
- Any content beyond this is not permitted and must be removed by a staff member.
- The limited purposes of the group, per the above, should be stated in the group – and that this is necessary for GDPR requirements, other legal requirements placed on the Organisation, and to comply with our insurance indemnity requirements.
- If INMO staff are members of instant messaging groups which are not established by the INMO, and they are a member of that group in their capacity as an INMO staff member, if the content and messages within the group go beyond the principles set out above then the staff member must remove themselves from the group.
- Groups should be deleted once there are no longer required.

Training and Awareness

INMO partners will be informed of the roll out of this policy, and it will also be available on our website.

Review

This policy will be reviewed in accordance with the frequency of review of the main Data Protection Policy. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.