Joseph Education University
ဂျိုးဇက်ပညာရေးတက္ကသိုလ်

Campus Address:
No. (739-741), Bagan Road (3), Quarter No. (123),
East Dagon 11451, Yangon, Myanmar.
Tel: 09426988746, 09777760001, 095040477
Email: jeupresident15@gmail.com
Website: www.jeiuniversity.com
ကျောင်းလိပ်စာ၊ အိမ်အမှတ် (၇၃၉-၇၄၁)၊ ပုဂံလမ်း (၃)၊ ရပ်ကွက် (၁၂၃)၊ အရှေ့ဒဂုံမြို့နယ် ၁၁၄၅၁၊ ရန်ကုန်။

Reg. No. 130581889

Data Protection Policy

1. INTRODUCTION

Joseph Education University ("the University") needs to collect and use personal data about its students, staff and other individuals who come into contact with the University. Those individuals ("data subjects") have privacy rights in relation to the processing of their personal data. Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

2. 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:

a. 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

- an identifier such as a name, an identification number, location data or online identifier, or
- 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.

c. 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

d. 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.

e. Data subject

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

f. 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. JEU, for example, is a data controller in relation to personal data relating to its own staff and students.

g. Data owner

Data owner means the most senior person in the department/school/college/administrative unit/research unit 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.

h. 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).

i. 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 organizations – 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 customer has 'opted in' to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the customer 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.

j. Members:

In this Policy, '**Members'** is used to refer to:

- any person who is employed or engaged by the University who processes personal data in the course of their employment or engagement;
- any student of the University who processes personal data in the course of their studies;
- Individuals who are not directly employed by JEU, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for JEU.

k. 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-

- the collection, recording, organization, structuring or storing of the data;
- the adaptation or alteration of the data;
- the retrieval, consultation or use of the data;
- the disclosure of the data by their transmission, dissemination or otherwise making the data available;
- the alignment or combination of the data; or
- the restriction, erasure or destruction of the data.

l. 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.

3. 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 membership
- 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 (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.

4. PURPOSE

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

5. SCOPE

5.1 What information is included in this Policy?

This policy applies to all personal data created or received in the course of University 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.

5.2 To whom does this Policy apply?

This policy applies to:

- any person who is employed or engaged by the University who processes personal data in the course of their employment or engagement;
- any student of the University who processes personal data in the course of their studies;
- individuals who are not directly employed by JEU, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for JEU.

Hereinafter these are collectively referred to as "Members".

5.3 Where does the Policy apply?

This policy applies to all locations from which University personal data is accessed, including home use.

6. DATA PROTECTION POLICY

The University undertakes to perform its responsibilities under the legislation in accordance with this policy.

6.1 Data Protection Principles

The University 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 minimization");**
• 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 JEU. 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 University 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 University 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.

Data Protection Notices

a. 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.

b. What needs to be included in a Data Protection Notice?

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

- who is collecting the data (e.g. Department of X, **University College Cork**);
- 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;

c. What rights people have in relation to their own data?

- 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.
- Further details on what information is required in a Data Protection Notice is contained within the Data Protection Notice Procedure.

Legal Basis for Processing

In order to collect and process personal data "lawfully", the University 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 are as follows:

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

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

****In cases where the University 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.

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

Members 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 minimization")*

Members 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")*

Members must ensure that the personal data being processed is accurate and, where necessary, kept up-to-date. Members 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")*

Members 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.

Members must comply with the University's Records Management Policy, and apply the University'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 organizational measures in order to safeguard the rights and freedoms of individuals.

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

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

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

Accountability

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 organizational measures that ensure and demonstrate that we comply;
- implement measures that meet the principles of privacy by design and by default such as:
    - data minimization;
    - pseudonymization;
    - transparency; and
    - creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate.
- record all data security breaches

6.2 Records of Processing Activities: Registers of Personal Data

In order to maintain documentation on processing activities, the University 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.

The University is also required to hold a register of personal data it holds where it acts as a **data processor**. Every department/unit/office in the University is required to record the information required to compile the Registers. This process is coordinated by the Information Compliance Manager. Nominated Data Protection Champions in each area are responsible for coordinating the compilation of the required information for their own area, in consultation with their Head of Department/Function. Heads of Department/Function must return the required information to the Information Compliance Manager. Heads must also notify the

Information Compliance Manager with details of any changes to the processing of personal data carried out in their area.

6.3 Privacy by Design and by Default

Privacy by Design states that any action an organization 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 University 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.

Members 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;
- Anonymizing personal data wherever necessary and appropriate.

6.4 Data Protection Impact Assessments (DPIA)

When JEU 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 minimizing those risks as far and as early as possible. It allows JEU to identify potential privacy issues before they arise, and come up with a way to mitigate them.

6.5 Personal Data Security Breaches

The University will take all necessary steps to reduce the impact of incidents involving personal data by following the University'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 Information Compliance Manager will liaise with the Data Protection Commissioner's Office and report the breach within 72 hours of discovery. The Information Compliance Manager will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach. Members who discover a personal data security breach must immediately inform their Head of Department/Unit who will

contact the Information Compliance Manager following the above procedure. **It is important that all Members act quickly and report any suspected incident without delay.**

6.6 Data Subject Rights

a. 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.

b. 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 University, the recipient should forward it immediately to the University's Information Compliance Manager (contact details below) who will respond to the request on behalf of the University, consulting with staff in relevant offices/departments and taking into account the narrow exemptions set out in the legislation.

In certain circumstances, the University 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 University's Information Compliance Manager.

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

c. 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 University must respond to a request within one calendar month. In certain circumstances, the University can refuse a request for rectification. All requests for rectification of personal data should be notified to the Information Compliance Manager without delay who will advise further on the steps to be taken to respond to the request.

d. 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 University 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 Information Compliance Manager without delay who will advise further on the steps to be taken to respond to the request.

e. 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 University 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 University must respond within one calendar month.

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

f. 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 Information Compliance Manager.

g. 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.

6.7 External Data Processors

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

- the **Externally Hosted Personal Data Policy** and approval process must be followed
- where determined applicable by the University's Third Party Hosting Group, there must be a written contract between the University (as data controller) and the supplier of the service (as data processor).
- the supplier must be entered into JEU's register of data processors held by the Information Compliance Manager.

6.8 Marketing / Mailing Lists / Electronic Privacy Regulations

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, itemized 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 JEU) using such communications and electronic communications networks to communicate with customers, 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 guidance note is available here.

Where Members process personal data to keep people informed about University activities and events they must provide in each communication a simple way of opting out of further communications. Members are required to follow the Guide to Direct Marketing when seeking to send out marketing communications on behalf of the University.

6.9 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. If installing a CCTV system, the **purpose** for its use must be displayed in a prominent position.

Before installing a CCTV system in the University, Members must consult with the Office of Corporate & Legal Affairs (Information Compliance Manager) and a Data Protection Impact Assessment must be undertaken.

6.10 CHILDREN'S PERSONAL DATA

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

7. ROLES AND RESPONSIBILITIES

The University has overall responsibility for ensuring compliance with the Data Protection Acts. However, all employees who process personal data in the course of their employment and students of the University who process personal data in the course of their studies or where they are employed by the University are also responsible for ensuring compliance with the Data Protection Acts.

The University 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 University's Information Compliance Manager (contact details below) will assist the University and its staff in complying with the Data Protection legislation.

Specifically, the following roles and responsibilities apply in relation to this Policy:

a. All users of University information:

- Must complete relevant training and awareness activities provided by the University 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 school/function who must in turn report the incident immediately to the Information Compliance Manager, so that appropriate action can be taken to minimize harm;
- Must inform the University of any changes to the information that they have provided to the University in connection with their employment or studies (e.g. changes of address or bank account details).

b. University Management Team – Operations (UMTO):

- the UMTO is responsible for reviewing and approving this Policy as recommended by the Corporate Secretary;
- each member of UMTO is responsible for ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility;
- members of UMTO must, as part of the University's Annual Statement of Internal Control, sign a statement which provides assurance that their functional area is in compliance with the Data Protection Acts.

c. Corporate Secretary:

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

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

d. Heads of Function:

Heads of School/Function 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 to be responsible for coordinating Data Protection compliance matters within each of the areas under their remit;

- enabling the Information Compliance Manager to maintain a record of processing activities by compiling (along with the Data Protection Champions for their areas of responsibility), approving and returning the information required for the compilation of the Register of Personal Data to the Information Compliance Manager.

e. Information Compliance Manager:

The Information Compliance Manager is responsible for administrative matters at an institutional level in relation to data protection. The principal data protection duties of the Information Compliance Manager 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;
- organize targeted training and briefing sessions for JEU staff as required;
- provide advice and guidance to JEU staff on data protection matters;
- maintain a centrally-held register of the categories of personal data held by JEU;
- maintain records of JEU's compliance with the Data Protection Acts;
- maintain a list of nominated Data Protection Champions within each area of the University with responsibility for coordinating data protection matters within their own areas.

f. Nominated Data Protection Champions within Colleges/Schools/ Departments/Offices/Centers:

Every College/School/Department/Office/Centre within JEU which processes personal data is required to nominate a suitable member of staff to be responsible for coordinating Data Protection compliance matters within their respective area, such matters to include:

- being a point of contact for the Information Compliance Manager regarding Data Protection;
- compiling and maintaining the information required from their area for the University's Register of Personal Data;
- bringing relevant Data Protection/IT security matters to the attention of relevant staff in his/her area;
- participating in training in data protection/IT security where appropriate.

g. Staff, students and other Members of JEU:

All staff, students and other Members 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 jeopardize individuals' rights or risk a contravention of the Act;
- report all data security breaches to their manager immediately;
- contact the Information Compliance Manager if in any doubt.

8. BREACH OF THIS POLICY

If any breach of this Policy is observed, then disciplinary action may be taken in accordance with the University's disciplinary procedures (Principal Statute for staff) and Student Disciplinary Procedure for Students as amended or updated from time to time.

9. SUPPORTING POLICIES, PROCEDURES & GUIDELINES

This policy supports the provision of a structure to assist in the University'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 University's Information Compliance Manager (see contact details below).

10. Review and Amendment

This policy has been approved by the University Management Team – Operations (UMTO). Any additions or amendments to this or related policies will be submitted by the Corporate Secretary to the UMTO for approval or to whatever authority the UMTO may delegate this role.

The policy will be reviewed every three years by the Information Compliance Manager and Corporate Secretary in light of any legislative or other relevant developments.

11. Policy Adaption

- **This policy is adopted on 1st January 2022.**

12. DISCLAIMER

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

APPENDIX - A:

LAWFUL BASES FOR PROCESSING

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

1. **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.

2. **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.

3. **Necessary for compliance with a legal obligation**

JEU is required by statute to retain certain records, for example employment records, health & safety records, student date. This lawful basis will cover a lot of the University's data processing.

4. **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.

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

This may occur where JEU carries out a task in the public interest or in an exercise where official authority has been invested in JEU 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.

6. **Necessary for the legitimate interests of the controller or a third party**

The processing is necessary for JEU'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, for example:

- Explicit consent from the individual;
- Necessary for legal obligations of the controller as an employer insofar as it is authorized by Myanmar law or a collective agreement;
- Necessary to protect the 'vital interests of the data subject where the data subject is physically or legally incapable of giving consent;
- Data has been 'manifestly made public' by the data subject themselves;

APPENDIX - B:

CONDITIONS FOR CONSENT

The university outlines the conditions for consent:

1. Where processing is based on consent, the University 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 - C:

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 - D:

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	Student/Staff Nos.
National ID Card details/Nos.	Next of kin / dependent / family details
Photographs	CVs
Personal financial data (e.g. Bank account details, credit card Nos.)	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/students

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.

Reference: **University College Cork**