Policy for Data Protection and Processing

Institute for Optimum Nutrition

1. Introduction

1.1 The Institute for Optimum Nutrition (ION) ("the Institute") is committed to data protection by default and by design and supports the data protection of all those whim who it works, including, but not limited to staff, students, visitors, alumni, clinic clients, publication subscribers, and research participants. This policy sets out the accountability and responsibilities of the Institute, its staff and its students to comply fully with the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (the DPA) and recognises that handling personal data appropriately and in compliance with the data protection legislation enhances trust, is the right thing to do, and protects the Institute's relationship with all its stakeholders.

1.2 The Institute holds and processes personal data about individuals such as employees, students, graduates, and others, defined as 'data subjects' by the law. Such data must only be processed in accordance with the GDPR and the DPA.

1.3 The Institute has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with the GDPR and the DPA. However, responsibility for compliance and the consequences of any breaches cannot legally be transferred to the DPO but instead remains with the business area.

1.4 This policy covers the following areas:

- Purpose of the policy
- Scope of the policy
- Responsibilities under the policy
- Data protection by design and default
- Responsibility of management and data users
- Handling of personal data by students
- Data subject rights
- Internal data sharing
- Transfers of personal data outside the EEA
- Direct marketing
- Data protection training
- Data protection breaches

2. Purpose of policy

2.1 This policy sets out the responsibilities of the Institute, its staff, and its students to comply fully with the provisions of GDPR and the DPA. It is accompanied by a series of other policies which provide information and guidance on different aspects of data protection. These policies form the framework which everybody processing personal data should follow to ensure compliance with data protection legislation.

3. Scope

3.1 This policy applies to all staff and students in all cases where the Institute for Optimum Nutrition or its students are the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used.

4. Responsibilities under the policy

4.1 The Institute as data controller has a corporate responsibility to implement and comply with data protection legislation. This corporate responsibility is delegated to Data Stewards in each area.

4.2 Data Security

4.2.1 All users of personal data within the Institute must ensure that personal data is always held securely and not disclosed to any unauthorised third party either accidentally, negligently, or intentionally. The Policy and Schedule for Data & Records Retention, Policy for ICT Acceptable Use, Policy for Information Security Incident Management, and Policy for the Protection of Information of Mobile Devices and Encryption must be read in conjunction with this Data Protection Policy.

4.3 Privacy notices

4.3.1 When the Institute collects personal data from individuals, the requirement for 'fairness and transparency' must be adhered to. This means that the Institute must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data are processed. Any data processing must be consistent or compatible with that purpose.

4.4 Conditions of processing/lawfulness

4.4.1 In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

1. The data subject has given consent.
2. The processing is required due to a contract.
3. It is necessary due to a legal obligation.
4. It is necessary to protect someone's vital interests (i.e. life or death situation).
5. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. It is necessary for the legitimate interests of the controller or a third party.

4.4.2 For special categories of personal data, at least one of the following conditions must be met:

1. The data subject has given explicit consent.
2. The processing is necessary for the purposes of employment, social security, and social protection law.
3. The processing is necessary to protect someone's vital interests.
4. The processing is carried out by a not-for-profit body.

5. The processing is manifestly made public by the data subject
6. The processing is necessary for legal claims
7. The processing is necessary for reasons of substantial public interest.
8. The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
9. The processing is necessary for public health
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards which are explained in the Handbook

4.5 Data retention

4.5.1 Personal data must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops, or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted.

5. Data protection by design and default

5.1 Under the GDPR and the DPA, the Institute has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measure to minimise the potential negative impact processing can have on the data subjects' privacy.

5.2 Data protection impact assessment

5.2.1 When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce privacy risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an after-thought.

5.2.2 A DPIA is:

- A tool/process to assist organisations in identifying and minimising the privacy risks of new projects, systems or policies
- A type of impact assessment conducted by an organisation, auditing its own processes to see how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes
- A tool/process to assist organisations in ensuring that all activities involving personal data are proportionate and necessary

5.2.3 A DPIA is designed to accomplish three goals:

- Ensure compliance with applicable legal, regulatory, and policy requirements for privacy;
- Determine the risks and effects; and
- Evaluate protections and alternative processes to mitigate potential privacy risks.

5.2.4 When do I need to carry out a DPIA?

5.2.4.1 When you plan to:

- Embark on a new project involving the collection of personal data;
- Introduce new IT systems for storing and accessing personal information;
- Participate in a new data-sharing initiative with other organisations;
- Initiate actions based on a policy of identifying particular demographics;
- Use existing data for a "new and unexpected or more intrusive purpose";
- Review or audit an existing system or activity.

5.3 Anonymisation and pseudonymisation

5.3.1 Further mechanisms of reducing risks associated with handling personal data are to apply anonymisation or pseudonymisation. Wherever possible, personal data must be anonymised or, where that is not possible, pseudonymised.

6. Responsibilities of management data users

6.1 Heads of departments, divisions, and teams have a responsibility to ensure compliance with the GDPR, the DPA and this policy, and to develop and encourage good information handling practices within their areas of responsibility. All users of personal data within the Institute has a responsibility to ensure that they process the data in accordance with the conditions set down in the legislation.

6.2 Every division must nominate one or more Data Protection Champion. These individuals are the first point of contact for data protection questions in their area, escalate difficult questions to the Data Protection Officer and act as a channel of communication between the Data Protection Officer and their area. Heads of departments may choose to delegate the management of, but not the responsibility for, data protection matters to their Division Data Protection Champion. The DPO will perform periodic audits to ensure compliance with this policy and the legislation

7. Handling research data

7.1 Before commencing any research which will involve obtaining or using personal data and special categories of personal data, the researcher must give proper consideration to this policy and the guidance contained in the Handbook and how these will be properly complied with. The researcher must ensure that the fairness, transparency and lawfulness principle is complied with and that privacy by design and default is applied. This means that wherever feasible, research data must be anonymised or pseudonymised at the earliest possible time.

8. Handling of research data by students

8.1 The use of personal data by students is governed by the following:

8.1.1 Where a student collects and processes personal data in order to pursue a course of study with the Institute, and this course of study is not part of a Institute-led project, the student rather than the Institute is the data controller for the personal data used in the research.

8.1.2 However, the domestic use exemption applies – if the data is extracted from a database already held by the Institute, the Institute remains the data controller for the database, but the student will be the data controller for the extracted data.

8.1.3 Once a thesis containing personal data is submitted for assessment, the Institute becomes data controller for that personal data.

8.1.4 Where a research student processes personal data whilst working on a project led by a Institute research group, the Institute is the data controller.

8.2 Academic and academic-related staff must ensure that students they supervise are aware of the following:

8.2.1 A student should only use personal data for a Institute-related purpose with the knowledge and express consent of an appropriate member of academic staff.

8.2.2 The use of Institute-related personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be anonymised so that students are not able to identify the subject.

9. Data subject rights

9.1 The GDPR and the Act contain eight data subject rights the Institute must comply with – the rights to information, subject access, to rectification, to object, to erasure, to portability, to restrict processing and in relation to automated decision-making and profiling. These rights can be restricted for personal data used in research.

9.2 Subject access requests and the right to data portability

9.2.1 Individuals have the right to request to see or receive copies of any information the Institute holds about them, and in certain circumstances to have that data provided in a structured, commonly used and machine readable format so it can be forwarded to another data controller. The Institute must respond to these requests within four weeks.

9.3 Right to erasure, to restrict processing, to rectification and to object

9.3.1 In certain circumstances data subjects have the right to have their data erased. This only applies:

- where the data is no longer required for the purpose for which it was originally collected, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

9.3.2 In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

9.3.3 If personal data is inaccurate, data subjects have the right to require the Institute to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

9.3.4 Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

9.3.5 Individuals receiving any of these requests should not act to respond but instead should contact the Data Protection Officer immediately.

10. Data sharing

10.1 When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the data subjects.

11. Transfer of personal data outside the EEA

11.1 Personal data can only be transferred out of the UK when there are safeguards in place to ensure an adequate level of protection for the data.

11.2 Any transfer of personal data outside the EEA that uses the Standard Contractual Clauses (SCCs) as a safeguard will need to be evaluated and authorised by the Business Manager.

12. Direct marketing

12.1 Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For the Institute, this will include notifications about events, fundraising, selling goods or services.

Marketing covers all forms of communications, such as contact by post, fax, telephone, and electronic messages, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003 (PECR). The Institute must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

13. Data protection training

13.1 The Senior Management Team has agreed that it should be mandatory for all employed staff and self-employed staff working in training clinic and in research, to complete data protection training as arranged by the Business Manager.

14. Data protection breaches

14.1 The Institute is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction, or damage of the data. The Institute makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

14.2 Any data protection incident must be brought to the attention of the Institute's Data Protection Officer who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, the Institute is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it. Any member of the Institute's community who encounters something they believe may be a data protection incident must email the Data Protection Officer immediately using the contact details below.

15. The Data Protection Officer

15.1 The Data Protection Officer is responsible for advising the Institute on compliance with data protection legislation and monitoring its performance against it.

- Gareth Pritchard
- Business Manager
- gareth.pritchard@ion.ac.uk
- 020 864 7809