IEC Data Protection Policy

Introduction

The purpose of this document is to provide a policy statement regarding the Data Protection obligations of IEC. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

Rationale

IEC must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by IEC in relation to its staff, service providers and clients in the course of its activities. IEC makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by IEC. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by IEC. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Subject Access Request procedure, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

IEC as a Data Controller

In the course of its daily organisational activities, IEC acquires, processes and stores personal data in relation to:

- Employees of IEC
- Students of IEC
- Third party service providers engaged by IEC

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, IEC is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the designated staff member with responsibility for Data Protection is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by IEC, there is regular and active exchange of personal data between IEC and its Data Subjects. In addition, IEC exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with IEC's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that an IEC staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the designated staff member with responsibility for Data Protection to seek clarification.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the designated staff member with responsibility for Data Protection, and will be processed as soon as possible. It is intended that by complying with these guidelines, IEC will adhere to best practice regarding the applicable Data Protection legislation.

Lawful Processing of Data

IEC operates within the education industry. Given the nature of the service it provides, IEC collects significant amounts of personal data on student and staff (its Data Subjects), including, but not limited to, names, email addresses, physical addresses, financial information and health information. IEC also interacts with other institutes as part of its processing of personal data.

The General Data Protection Regulation states that data must be processed in a lawful manner. Specifically, it outlines the following six criteria, one of which must apply for an organisation or institute to have a lawful basis to process data. These six criteria are:

1. **Consent** – Where students have given full, free and explicit consent
2. **Contract** – Where processing is necessary to satisfy a contract with the student
3. **Legal Obligation** – Where processing is required to comply with an EU or member state legal obligation to which the HEI is subject
4. **Vital Interests** – Where processing is needed to protect the life of the data subject
5. **Public Interest** – Where processing is necessary for the public interest or in the exercise of an official authority vested in the data controller
6. **Legitimate Interests** – Where processing is necessary for the legitimate interests of the Educational establishment, in other words where data processing is required to enable the Educational establishment to carry out its core functions. This basis is only lawful if it does not override the fundamental rights and freedoms of the student.

To effectively fulfil its core functions, IEC does have a **legitimate interest** to process some personal information of its Data Subjects. For example, IEC must process personal data relating to assessment results to ensure that it fulfils a core function of facilitating its students with the opportunity to complete an official exit exam, in the evident that that student has successfully fulfilled all the requirements of a validated programme.

The data processing activities for which IEC can claim legitimate interest are:

- Processing of assessment information
- Incidents of academic impropriety
- Ensuring accessibility to course content
- Informing students of developments relevant to their programme of study and assessing level progression
- Recording minutes of formal meetings that are specified within IEC's quality assurance structures
- Maintenance of the student record (to provide insights on a student during the studies with IEC)

However, it is not sufficient to claim that legitimate interest can cover all aspects of the data processing done by IEC. For example, IEC may periodically use student data for statistical analysis of academic performance, to alert students to other programmes of study that it may think a specific learner will be interested in, or use staff feedback to inform reports. Neither of these examples would be covered by the legitimate interest criteria, and could not be considered critical to the effective provision of IEC's core functions. In such instances, IEC will seek **consent** for the processing of data from its data subjects.

The data processing activities for which IEC can claim legitimate interest are:

- Use of personal, anonymised data for statistical analysis purposes
- Use of personal data for communication purposes outside those that are core for the successful participation on an academic programme
- Use of personal comments or feedback on the programmes or services provided by IEC, with a view to using these in reports or as a basis for future improvements

Furthermore, in certain instances, IEC does process data in compliance with **legal obligations**. This is typically to ensure compliance with regulatory specifications, such as retention of data for specified periods, but is also required for its provision of international (non-EEA) students.

The data processing activities for which IEC can claim legitimate interest are:

- Retention of personal information of staff in line with regulatory requirements (see Data Retention Periods document)
- Providing personal information of non-EEA, students (who require a student visa) as requested by Garda National Immigration Bureau

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the IEC's Data Protection policy.

In its capacity as Data Controller, IEC ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data is being collected, be made aware of:

- The identity of the Data Controller (IEC)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

IEC will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, IEC will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where IEC intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of IEC's lawful activities, and IEC will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to IEC and operating on its behalf.

2. .... be obtained only for one or more specified, legitimate purposes.

IEC will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which IEC holds their data, and IEC will be able to clearly state that purpose or purposes.

3. ..... not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by IEC will be compatible with the purposes for which the data was acquired.

4. .... be kept safe and secure.

IEC will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by IEC in its capacity as Data Controller.

Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation and password access.

5. ***... be kept accurate, complete and up-to-date where necessary.***

IEC will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. IEC conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ***... be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.***

IEC will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. ***... not be kept for longer than is necessary to satisfy the specified purpose(s).***

IEC has identified an extensive reference list of data categories, with reference to the appropriate data retention period for each category. The list applies to data in both a manual and automated format.

Once the respective retention period has elapsed, IEC undertakes to destroy, erase or otherwise put this data beyond use.

8. ***... be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.***

IEC has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, IEC's staff engages in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by IEC, such a request gives rise to access rights in favour of the Data Subject.

The Data Subject is entitled to the following information as part of a subject access request:

- A copy of their personal data
- The purposes for processing the data.
- The categories of personal data concerned.
- To whom the data has been or will be disclosed.
- Whether the data has been or will be transferred outside of the EU.
- The period for which the data will be stored, or the criteria to be used to determine retention periods.
- The right to make a complaint to the Data Protection Commissioner.
- The right to request rectification or deletion of the data.

- Whether the individual has been subject to automated decision making.

The Data Subject is also entitled to have inaccurate data corrected, should this materialise as part of a subject access request. Data Subjects can apply to have their information changed or deleted where that information:

- is factually incorrect;
- was obtained or processed in an unfair way;
- is not accurate, complete or up to date;
- is being used in a manner incompatible with the reason for which it was originally collected.;
- is being stored in an unsafe way, or where storage security measures are inappropriate; or
- the organisation cannot provide a valid reason for retaining it.

Both a subject access request and a request to correct erroneous information will carry **no fee.**

IEC, as a data controller, does have the right to refuse a data access request if it is deemed that such a request is manifestly unfounded or excessive. The criteria that can lead to IEC refusing a data access request are as follows:

- An individual makes a data access request for information that is not their own, and for which they do not have permission from the Data Subject
- If data is subject to legal privilege
- Where an individual is involved in a claim against IEC
- Where information relating to third parties would be disclosed
- Where the data being sought involves personal opinions expressed by another individual and given in confidence

There are specific time-lines within which IEC must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request procedure document.

IEC's staff will ensure that, where necessary, such requests are forwarded to the designated individual with responsibility for Data Protection, in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 28 days from receipt of the request. The Data Subject is entitled to receive a copy of their personal data in printed, oral or electronic format, as per their own specific preference.

Implementation

As a Data Controller, IEC ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage IEC's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of IEC's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, IEC refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by IEC to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.