THE INSTITUTE OF EDUCATION

The Institute of Education,
79-85 Lower Leeson Street, Dublin 2, Ireland.
Tel: +353 1 661 3511
Email: info@instituteofeducation.ie
www.instituteofeducation.ie

The Institute of Education Data Protection Policy

March 2022
v.3

1.0 Introduction

1.1 The purpose of this Data Protection Policy is to support The Institute of Education (hereby referred to as “The Institute”, “we”, “our”, “us”) in meeting its responsibilities with regard to the processing of personal data. These responsibilities arise as statutory obligations under the relevant data protection legislation. They also stem from our desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons.

1.2 This policy aims to help transparency by identifying how The Institute expects personal data to be treated (or “processed”). It helps to clarify what data is collected, why it is collected, for how long it will be stored and with whom it will be shared.

1.3 The Data Protection Act 2018 and the General Data Protection Regulation (“**GDPR**”) are the primary legislative sources. As such they impose statutory responsibilities on The Institute as well as providing several rights (for students, parents/guardians and staff and others) in relation to personal data.

1.4 The Institute recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. This Data Protection Policy applies to all Institute staff, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within The Institute).Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action.

1.5 Any amendments to this Data Protection Policy will be communicated through The Institute website and other appropriate channels, including direct communication with data subjects where this is appropriate.

2.0 Definitions

2.1 Data – any information in a form that can be processed.

Personal Data – data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the Controller.

- *Sensitive Data* – data relating to a person’s
- Race or ethnic origin, political opinions, religion or philosophical beliefs
- Trade union membership
- Genetic or Biometric data
- Health data or sexual orientation

Controller – Is a natural or legal person who alone or with others determines the purpose and means of the processing of personal data. The Institute is the controller.

Data Subject - a living, identified or identifiable individual about whom we hold Personal Data.

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.

Processor – Is a natural or legal person which processes data on behalf of the controller.

Processing – an operation or set of operations which is performed on personal data. This can be collection, recording, organisation, structuring, storage, altering, retrieval, use, disclosure, circulation, restriction, erasure or destruction. Processing can include any activity that might relate to personal data under the control of the Institute, including the storage of personal data, regardless of whether the records are processed by automated or manual means.

3.0 Processing Principles

3.1 In order for the use of personal data to be lawful, it should be processed on the basis of a legal basis as set out under Articles 6 and 9 GDPR.

The Institute of Education will ensure that your data is processed fairly and lawfully in keeping with the principles of data protection and will process personal data under various legal bases depending on the purpose for which the data is collected.

- Where The Institute is required to process personal data by law or for complying with employment law.
- Where the processing of personal data is necessary for the formation of a contract with students and their parents.
- Where the processing of personal data is related to the delivery of The Institute services, we may sometimes process personal data based on legitimate interests e.g. for the administration and delivery of classes and the use of support services.
- In other instances, we may seek consent from the data subject.

3.2 There are a number of fundamental principles, set out in the data protection legislation, that legally govern our treatment of personal data. As an integral part of its day to day operations, The Institute will ensure that all data processing is carried out in accordance with these processing principles.

3.3 These principles, set out in the GDPR, establish a statutory requirement that personal data must be:

(i) processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (purpose limitation);

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization);

(iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);

(v) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation);

(vi) 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);

(vii) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

(viii) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

3.4 GDPR also establishes Accountability as a core data processing principle. This places a statutory responsibility on The Institute, as Data Controller, to be able to demonstrate compliance with the other principles i.e. the data processing principles set out in the previous paragraph (3.00 above).

4.0 Managing Personal Data

The Institute will collect and process personal data fairly, in line with the purpose for which you provide it and to the extent necessary to provide you with the information or service you require. The Institute is satisfied that the data which it holds is adequate, relevant and not excessive for the purpose for which it has been obtained.

If The Institute plans to use this personal data for future purposes this will be brought to the individual's attention at the time of collection. Individuals will be given the option of saying whether or not they wish their data to be used in these other ways. If The Institute has data and wishes to use this for a new purpose (which was not disclosed at the time the data was collected), individuals will be given an option to decline or op out, except in exceptional circumstances whereby The Institute is obliged by law to disclose the data or is permitted by law to use this data in this manner without the consent of the individual.

The Institute is satisfied that the necessary measures are in place to prevent unauthorised access to, alteration of, disclosure of or destruction of the data and against its accidental loss.

The personal data collected and retained by The Institute may include but are not limited to:

Student records

- Student name, address, contact details, date of birth
- Parent/guardian name, address and contact details
- Previous educational details
- Previous attendance record
- Previous disciplinary record
- Previous academic records (including reports, references, assessments and other relevant records)
- Relevant special requirements e.g. Medical or special educational needs
- Junior Cycle or Leaving Certificate results
- Passport photograph
- Psychological or medical assessments
- Any relevant exemptions
- Garda Vetting record e.g. work experience organised with or through The Institute which requires that they be Garda vetted
- Recording of classes

The grounds for seeking, retaining and processing student records is as follows:

- Facilitate the management and administration of Institute business

- To comply with legislative or administrative requirements
- To ensure that students meet the entry criteria and age requirements
- To provide educational, emotional, and physical support to enable each student to reach their full potential
- To enable parents/guardians to be contacted in the case of emergency or in the case of Institute closure
- To provide the parent/guardian on information relating to their student's attendance and educational progress
- To celebrate Institute achievements, compile yearbooks, establish The Institute website, record Institute events and to keep a record of the history of The Institute
- To provide information on other relevant courses that may assist the student
- To ensure the safety and wellbeing of the student
- To send on any information to the Department of Education, the National Council for Special Education, TUSLA or other bodies in compliance with the law and directions issued by government departments
- To complete documentation, references, application forms as requested by the students or parents/guardians to third level institutions and/or prospective employers.
- To ensure delivery of course material is optimised for the student to improve educational experiences, particularly, providing students with the ability to review and revise specific aspects of the class experience.

Student data is kept in both manual form within a secure filing system, and The Institute management system on computer files. The computer files and Institute management system require a username and password and our employees are required to maintain the confidentiality of any data to which they have access. It is the responsibility of parents/guardians to inform The Institute of any change to their son or daughter's data.

Parent/Guardian Records

- Name, address & contact details
- Financial information
- Relationship to student
- Correspondence

The grounds for seeking, retaining and processing parent/guardian records is as follows:

- Facilitate the management and administration of Institute business
- To provide communication on students, attendance (daily & class), class tests, parental portal, academic reports, Institute events
- To provide information on other relevant courses that may assist the student
- To provide financial information such as statements, invoices, receipts
- In case of emergency

It is the responsibility of the parent/guardian to inform The Institute of any change to their data.

Staff records

These records may include but not limited to the following:

- Name, address and contact details
- PPS number
- Emergency contact details

- Medical issues (voluntarily disclosed to The Institute)
- Original CV and/or application form
- Employment Contract
- Garda Vetting details
- Details of absences, sick days, annual leave, parental leave etc
- Details of performance reviews
- Employee Job Descriptions
- Details of any accident/injury sustained on Institute property or in connection with a staff member
- Record of any reports The Institute (or its employees) have made in respect of the staff member
- Salary information
- Recording of classes

The grounds for seeking and retaining staff records is as follows:

- To facilitate the management and administration of Institute business
- To manage human resources
- To facilitate the payment of staff and calculate other entitlements
- In the event of an emergency, emergency contact details are held on file.
- To record promotions made and changes in role and responsibilities etc.
- To enable The Institute to comply with its obligations as an employer under the Safety, Health and Welfare At Work Act 2005
- For compliance with legislation for the Institute
- Recording of classes

Staff data is kept in both manual form within a secure filing system, and on The Institute management system and on computer files. The computer files and Institute management system require a username and password and our employees are required to maintain the confidentiality of any data to which they have access. It is the responsibility of the employee to inform The Institute of any change to their data.

Third Parties

The Institute may hold some or all of the following information on individuals that do business with

The Institute

- Name
- Address
- Contact Details
- PPS Number
- Tax details
- Bank Account details
- Invoices
- Delivery docket

This information is needed for routine management and administration of The Institute's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

5.0 CCTV

The purpose of the CCTV System Policy in The Institute of Education is to regulate the management, operation and use of the closed circuit television (CCTV) system in the school environs. All CCTV monitoring equipment is held in a secure area with restricted access to authorised personnel only. Unauthorised access to that area when it is unoccupied will not be permitted and this area will remain locked when unoccupied by the authorised personnel. In certain circumstances, CCTV footage may be accessed for the following reasons

- To facilitate the management and administration of Institute business
- By the Principal, the Deputy Principal, administration staff or teachers in order to assist in establishing facts about a case of theft of a student's property or unacceptable behaviour of a student, after which the students' parents/guardians will be informed.
- By An Garda Siochána as requested by them or where the Institute is required by law to inform them of a crime committed or where it is suspected that anti-social/illegal behaviour is taking place in Institute property
- By individuals subject to a court order or warrant
- By The Institute's insurance company where the insurance company requires access in order to pursue a claim for damage done to the Institute property or health and safety reasons.

6.0 Data Sharing Guidelines

(i) From time to time The Institute may disclose Personal Data to third parties, or allow third parties to access specific personal data under its control. An example could arise should Gardai submit a valid request under Section 41(b) of the Data Protection Act 2018 which allows for processing necessary and proportionate for the purposes of preventing, detecting, investigating or prosecuting criminal offences.

(ii) In all circumstances where personal data is shared with others, The Institute will ensure that there is an appropriate lawful basis in place (GDPR Articles 6, 9 as appropriate). We will not share information with anyone without consent unless another lawful basis allows us to do so.

(iii) Most data transfer to other bodies arises as a consequence of legal obligations that are on The Institute, and the majority of the data recipients are controllers in their own right, for example, the Department of Education and Skills. As such, their actions will be governed by the GDPR and Data Protection Act 2018.

(iv) Some of The Institute's operations require support from specialist service providers. For example, The Institute may use remote IT back up and restore services to maintain data security and integrity. In cases such as these, where we use specialist data processors, we will ensure that the appropriate security guarantees have been provided and that there is a signed processing agreement in place. The Data Protection Policy of the Department of Education and Skills can be viewed on its website (www.education.ie).

7.0 Personal Data Breaches

Consequences of a Data Breach

(i) A breach can have a significant adverse effect on individuals, which can result in physical, material or non-material damage. This can include discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality etc. Children because of their age may be particularly impacted.

(ii) In addition to any detrimental impact on individual data subjects, a data breach can also cause serious damage to The Institute. This can include reputational damage as well as exposing The Institute to other serious consequences including civil litigation.

(iii) It should be noted the consequences of a data breach could include disciplinary action, criminal prosecution and financial penalties or damages for The Institute and participating individuals.

7.1 Responding to a Data Breach

(i) The Institute will always act to prioritise and protect the rights of those individuals whose personal data is affected.

(ii) As soon as The Institute becomes aware that an incident has occurred, measures will be taken to assess and address the breach appropriately, including actions to mitigate any possible adverse effects.

(iii) Where the Institute believes that there is a risk to the affected individuals, the Institute will (within 72 hours of becoming aware of the incident) submit a report to the Data Protection Commission.

(iv) Where a breach is likely to result in a high risk to the affected individuals, The Institute will inform those individuals without undue delay.

Data Access

All data is stored in a secure environment at The Institute. The storage areas are locked when unoccupied by authorised personnel.

Access to our Institute management system requires a username and password and the data is restricted depending on the employee's access level. We have backup procedures for all computer held data.

Data Request

The GDPR provides for right of access by an individual data subject to personal information held by the Institute. It is requested that persons making a request, do so in writing, and by completing the Data Subject Request Form. This may apply to a staff member or student seeking information on his or her own behalf or maybe a parent/guardian seeking information on behalf of his or her own son/daughter. There is no automatic right of a parent/guarding to a copy of information relating to their child. No information will be given out that relates to another individual.

Others making an access request

On making an access request, any individual about whom The Institute keeps personal data, is entitled to:

- A copy of the data which is kept about him/her (unless the GDPR or Data Protection Act 2018 precludes The Institute from providing same, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Commission).
- Know the purpose/s for processing his/her data;
- The categories of personal data concerned;
- Know the identity of those to whom the data is disclosed;
- The envisaged retention period for which the personal data will be stored, or, if not possible the criteria used to determine that period;

- The right to request from The Institute rectification or erasure of personal data or restriction of personal data concerning the data subject or to object to processing;
- The right to lodge a complaint with the Data Protection Commission;
- Know the source of the data, unless it is contrary to public interest;
- The existence of automated decision-making, including profiling.

Data Request Procedure

It requested that the data subject apply in writing requesting access to the data and complete the Data Subject Request Form which will help The Institute in processing the access request more quickly.

- The Institute reserves the right to request official proof of identity e.g. photographic ID such as a driver's license or passport where there is any doubt on the issue of identification.
- On receiving the Data Access Request Form the GDPR officer will check the validity of the access request and check that sufficient information to locate the data has been supplied. It may be necessary for the GDPR officer to contact the data subject if further information is required.
- The Data Access Request and a log of all steps taken to provide the data will be recorded in the Subject Matter Request Register.
- The GDPR Officer will make sure that all relevant manual files, spreadsheets and computer systems are checked for the data in respect for which the request is made.
- The GDPR Officer will make sure that the information is supplied within one month after the request was made, or, where not feasible to do so, update the data subject as to the status of the request and provide an estimate of when the request will be complied with.
- Where a request is made the following information will be supplied
  – The personal information that The Institute holds on the data subject
  – A description of the data with details of the purpose of retention of this data
  – Be advised the identity of those whom has access to this data
- Actual copies of the personal data will not be given and no personal data can be supplied to another individual.
- All requests regarding State Examination Results must go directly to the State Examinations Commission in Athlone.
- If data relating to a 3rd party is involved, it will not be disclosed without the prior consent of the 3rd party.
- The Institute reserves the right to seek legal advice where they may be unsure as to what information they can disclose.
- The GDPR Officer will ensure that the information provided is legible, where possible.
- The GDPR Officer will sign off on the data supplied.
- Where another data access request has been made after the first request has been compiled with, The Institute has discretion as to what constitutes a reasonable interval between access requests and this will be done on a case-by case basis.
- Where a data subject may ask to rectify incorrect information held by The Institute, he/she should notify The Institute complete a form supplied.
- In a circumstance where the access request is denied The Institute will write to the data subject to explain why this was denied. In such circumstances the data subject has the right to make a complaint to the Data Protection Commission www.dataprotection.ie.
- When a request is made for CCTV footage, it is requested that an application be made in writing and the timeframe for response is within one month of receiving the request, or, if not feasible to provide the information within that timeframe, an extension of one month may be applied. In providing a copy of personal data The Institute may provide the materials in the form of a still/series of pictures, a disc or a USB. Other people's images will be obscured before the data is released. If other people's images may not be obscured than the images will/may not be released.

Data Subject Rights

Your Rights Personal Data will be processed by The Institute in a manner that is respectful of the rights of data subjects. Under GDPR these include:

- the right to information
- the right of access
- the right to rectification
- the right to erasure ("right to be forgotten")
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision making
- the right to withdraw consent
- the right to complain.

7.2 **Right to be Informed:** You are entitled to information about how your personal data will be processed. We address this right primarily through the publication of this Data Protection Policy. Should you seek further clarification, or information that is not explicit in our Policy or Privacy Statements, then you are requested to forward your query to The Institute.

7.3 **Right of Access**: You are entitled to see any information we hold about you. The Institute will, on receipt of a request from a data subject, confirm whether or not their personal data is being processed. In addition, a data subject can request a copy of their personal data. The Institute in responding to a right of access must ensure that it does not adversely affect the rights of others. If you are a student who is subject to estimated marks, and you make a data access request to The Institute for your estimated marks before the issue of results, The Institute will advise the following:

- that in line with section 56 of the Data Protection Act, it is not possible to respond to the request at present, and
- that the request will be taken to have been made on the later of either the date of the first publication of the results of the 'examination' (i.e. the Accredited Grades process), or the date of the request.

7.4 **Right to rectification:** If you believe that The Institute holds inaccurate information about you, you can request that we correct that information. The personal record may be supplemented with additional material where it is adjudged to be incomplete.

7.5 **Right to be forgotten:** Data subjects can ask The Institute to erase their personal data. The Institute will act on such a request provided that there is no compelling purpose or legal basis necessitating retention of the personal data concerned.

7.6 **Right to restrict processing**: Data subjects have the right to seek a restriction on the processing of their data. This restriction (in effect requiring the controller to place a "hold" on processing) gives an individual an alternative to seeking erasure of their data. It may also be applicable in other circumstances such as where, for example, the accuracy of data is being contested.

7.7 **Right to data portability**: This right facilitates the transfer of personal data directly from one controller to another. It can only be invoked in specific circumstances, for example, when processing is automated and based on consent or contract.

7.8 **Right to object:** Data subjects have the right to object when processing is based on The Institute's legitimate interests or relates to a task carried out in the public interest (e.g. the processing of CCTV data may rely on The Institute's legitimate interest in maintaining a safe and secure Institute building). The Institute must demonstrate compelling legitimate grounds if such processing is to continue.

7.9 **Right not to be subject to automated decision making:** This right applies in specific circumstances (as set out in GDPR Article 22).

7.10 **Right to withdraw consent:** In cases where The Institute is relying on consent to process your data, you have the right to withdraw this at any time, and if you exercise this right, we will stop the relevant processing.

7.11 **Limitations on Rights:** While The Institute will always facilitate the exercise of your rights, it is recognised that they are not unconditional: The Institute may need to give consideration to other obligations.

7.12 Right to Complain

(i) If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Principal who is responsible for operational oversight of this policy.

(ii) A matter that is still unresolved may then be referred to The Institute's Data Controller by writing to The Institute's School Principal.

(iii) Should you feel dissatisfied with how we have addressed a complaint or concern that you have raised, you have the right, as data subject, to bring the matter to the attention of the Data Protection Commission (https://www.dataprotection.ie/).

8.0 Retention of Data

The Institute, in its role as a Data Controller, is conscious of its statutory obligations to be full transparent in relation to the length of time for which personal data will be kept. The Institute has put in place procedures to ensure compliance with all directives in relation to the storing and retention of data sought by The Institute.

The Institute of Education reserves the right to review or amend this policy at any time.