



# The Institute of Education

## Data Protection Policy

### General Statement

The Institute of Education fully respects your right to privacy and actively seeks to preserve the privacy rights of those who share information with us. This includes respect for the protection of data collected and stored at the school and for the right of access to this data. This policy is informed by the Data Protection Act of 2016/679. It applies to all staff, teachers, parents/guardians, students (including prospective students) and their parents/guardians.

### Definitions

*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 Data Controller.

*Sensitive Data* – data relating to a persons

- 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 of Education is the controller.

*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.

## **Managing Personal Data**

The Institute of Education 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 school is satisfied that the data which it holds is adequate, relevant and not excessive for the purpose for which it has been obtained. The personal data may be disclosed to staff and teachers in order to support services to you.

If the school 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 school 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 opt out, except in exceptional circumstances whereby the school 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 of Education 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.

At The Institute of Education the personal data collected and retained by the school may include but are not limited to:

### **Student records**

- Student name, address, contact details, date of birth, nationality
- 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 Certificate 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 school which requires that they be Garda vetted
- CCTV

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

- Facilitate the management and administration of school 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 school closure
- To provide the parent/guardian on information relating to their student's attendance and educational progress
- To celebrate school achievements, compile yearbooks, establish the school website, record school events and to keep a record of the history of the school
- 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 keep students informed of future courses.

Student data is kept in both manual form within a secure filing system, on our school management system and on computer files. The computer files and school 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 school 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 school business
- To provide communication on students, attendance (daily & class), class tests, parental portal, academic reports, school 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 school of any change to their data.

**Staff records** – these records may include:

- Name, address and contact details
- PPS number
- Original CV and/or application form
- Contract
- Details of absences, sick days, annual leave, parental leave etc
- Details of performance reviews
- Record of subjects & classes taught

- Details of any accident/injury sustained on school property or in connection with a staff member
- Record of any reports the school (or its employees) have made in respect of the staff member
- CCTV

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

- To facilitate the management and administration of school business
- To manage human resources
- To facilitate the payment of staff and calculate other entitlements
- To record promotions made and changes in role and responsibilities etc
- To enable the school to comply with its obligations as an employer under the Safety, Health and Welfare At Work Act 2005
- For compliance with legislation to the school

Staff data is kept in both manual form within a secure filing system, on our school management system and on computer files. The computer files and school 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 school of any change to their data.

### **3<sup>rd</sup> Parties**

The school may hold some or all of the following information on companies that do business with the school

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

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

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

### **CCTV**

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:

- To facilitate the management and administration of school 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 Síochána as requested by them or where The Institute of Education 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 school property
- By individuals subject to a court order
- By the schools insurance company where the Insurance Company requires access in order to pursue a claim for damage done to the school property

### **Data Access**

At The Institute of Education all data is stored in a secure environment. The storage areas are locked when unoccupied by authorised personnel.

Access to our school 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 Data Protection Act 2016/679 provides for right of access by an individual data subject to personal information held by The Institute of Education. They must apply in writing 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. No information will be given out that relates to another individual.

#### **Student Access Requests**

Where a student aged under 18 years makes a data access request, the school will inform the student that:

- Their parents will be informed that they have done so
- A copy of the access request materials being supplied to the data subject by the school will also be sent to the student's parent/guardian

There may be some data held by the school which may be of a sensitive nature and the school will have regard to the following guidance issued by the Office of the Data Protection

Commissioner in relation to releasing such data:

- A student aged eighteen years or older (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged eighteen years or older has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.

While a student aged from twelve up to and including seventeen can be given access to their personal data, depending on the age of the student and the nature of the record i.e. it is suggested that:

- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access.

- If the information is of a sensitive nature, parental/guardian consent will be sought before releasing the data to the student.
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student.

#### Parent Access Requests on behalf of their son/daughter

Where a parent/guardian makes an access request on behalf of their son/daughter (a student under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the daughter, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the student is registered on the school's records and will be addressed to the son/daughter. Where a parent/guardian is unhappy with this arrangement, the parent/guardian is invited to make an application to court under section 11 of the Guardianship of Infants Act 1964. This provision enables the court (on application by a guardian) to make a direction on any question affecting the welfare of the child. Where a court issues an order stating that a school should make certain information available to a parent/guardian, a copy of the order should be given to the school by the parent/guardian and the school can release the data on foot of the court order.

#### Others making an access request

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

- A copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Commissioner).
- Know the purpose/s for processing his/her data.
- Know the identity of those to whom the data is disclosed.
- Know the source of the data, unless it is contrary to public interest.

#### **Data Request Procedure**

- The Data Subject must apply in writing requesting access to the data and complete the Data Subject Request Form which will help the school in processing the access request more quickly.
- The school reserves the right to request official proof of identity e.g. photographic id such as a drivers licence 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 30 days after the request was made.
- Where a request is made the following information will be supplied

- The personal information that the school 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 3<sup>rd</sup> party is involved, it will not be disclosed without the prior consent of the 3<sup>rd</sup> party.
- The school 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 school 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 school, he/she should notify the school complete a form supplied.
- In a circumstance where the access request is denied The Institute of Education 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 Commissioner [www.dataprotection.ie](http://www.dataprotection.ie).
- When a request is made for CCTV footage an application must be made in writing and the timeframe for response is within 30 days. In providing a copy of personal data the school 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.

### **Right of Rectification**

The data subject has the right to request from the controller the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed.

### **Right to be Forgotten**

The data subject shall have the right to request, from the controller (Institute of Education) the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject withdraws consent on which the processing is based and where there is no other legal or overriding legitimate grounds for the processing
- the personal data has been unlawfully processed
- the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject

### Opt Out of future course communications

Students & Parents may choose to opt out from receiving any communications related to other courses & programmes provided by the school by completing the form here:

<https://www.instituteofeducation.ie/gdpr/>

### Retention of Data

The Institute of Education, 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 of Education has put in place procedures to ensure compliance with all directives in relation to the storing and retention of data sought by the school.

Below are listed guidelines to the length of time various categories of data are stored at the school:

Student Records	Retention period	Disposal
Registration form – Full Time	Indefinitely	Archive
Registration form – Part Time	Indefinitely	Archive after 10 years
Financial records – Full Time	7 Years Post Leaving Certificate	Deletion & Confidential shredding
Financial records – Part Time	7 Years Post Leaving Certificate	Deletion & Confidential shredding
Application form – Full Time - not accepted/declined place	7 Years Post Leaving Certificate	Archive
Attendance records – Full Time	7 Years Post Leaving Certificate	Deletion
Attendance records – Part Time	7 Years Post Leaving Certificate	Deletion
State Exam results – Paper copy	1 Year Post Leaving Certificate	Confidential shredding
State Exam results – Digitalised – (student consent given)	Indefinitely	Archive after 1 year post Leaving Certificate
In house academic reports	7 Years Post Leaving Certificate	Deletion & Confidential shredding
Psychological/Medical Reports	7 Years Post Leaving Certificate	Confidential shredding
Special Accommodation needs	7 Years Post Leaving Certificate	Confidential shredding
Record of school trips/tours	Indefinitely	Archive
Accident Reports	7 Years Post Leaving Certificate	Confidential shredding
Moodle	3 Years after registration	Archive
CCTV	6 Months	Automatic deletion
Student Questionnaires	Indefinitely	Deletion & Confidential shredding



Staff Records	Retention period	Disposal
Personnel file e.g. cv, application, references, contract, training, reviews etc	Indefinitely	Archive
Interview material	Indefinitely	Archive
Staff rates	Indefinitely	Archive
New employee form	Indefinitely	Archive
Disciplinary documentation	Indefinitely	Archive
Conflict documentation	Indefinitely	Archive
Sick & annual leave	Indefinitely	Archive
Leave of absence e.g. maternity/paternity, parental leave, career break	Indefinitely	Archive
Allegations/complaints	Indefinitely	Archive
Garda Vetting	5 Years	Deletion or if still currently employed will need updating
CCTV	6 Months	Automatic deletion

If data remains relevant it is moved to archives. Paper copies and print outs etc are disposed of using the in house shredding facility. When computers are decommissioned the hard drive is destroyed.

### Changes to our Privacy Policy

Any changes we may make to our privacy policy in the future will be posted on this page and will be effective upon posting and as reflected in the 'Last Revised' date shown in the revised policy. You should regularly check back to this page to see any updates that may have been made.

If you have any queries relating to this policy, please email [gdpr@instituteofeducation.ie](mailto:gdpr@instituteofeducation.ie).