



EMPLOYEE PRIVACY POLICY

ORGANISATION:	Loreto Secondary School, Wexford
LOCATION:	Pembroke Hill, Ballynagee, Wexford
AUTHORISED BY:	Board of Management of Loreto Secondary School, Wexford
AUTHORISED DATE:	14 th February 2022

The school collects and processes personal data relating to its employees to manage the employment relationship. The school is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the school collect?

The school collects and processes a range of information about you.

This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the school;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in Ireland;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and the reasons for the leave;

- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the school needs to make reasonable adjustments;
- details of trade union membership;
- images and videos of you during participation in school activities and events;
- images recorded on CCTV (not used for the purposes of staff monitoring); and
- details relating to your health in relation to having any potential symptoms of Covid-19.

The school collects this information in a variety of ways. For example, data is collected through application forms, CVs; from correspondence with you; or through interviews, meetings or other assessments.

Data is stored in a range of different places, including in your personnel file, and in IT systems (including the school's email system), with access controls in place

How does the school collect personal data?

The school collects this information in a variety of ways. For example, data is collected through:

- application forms;
- CVs;
- correspondence with you;
- through interviews, meetings or other assessments;
- generally through the course of your work; and
- through CCTV or video or photos.

Why does the school process personal data?

The school needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer any relevant benefits.

In some cases, the school needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in Ireland and to deduct tax.

In other cases, the school has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

Processing employee data allows the school to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes;
- operate and keep a record of employee absences;

- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental leave), to ensure that the school complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims;
- maintain and promote equality in the workplace;
- ensure the safety and security of staff through CCTV but recording are not used for staff monitoring;
- to promote the school through the school website and app by celebrating achievements; and
- to protect the health and safety of all staff and students by recording details of any symptoms of Covid-19 and to meet the guidelines of Public Health Authorities.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Who has access to data?

Your information will be shared internally with relevant staff and Board members when necessary in the performance of their duties and is kept strictly confidential at all times. The school has a legal obligation to share your information with the Department of Education and Skills as well as with other state agencies such as the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies.

The school also shares your data with third parties in the form of IT support contractors, and other professional service contractors where this may be necessary in the performance of their contracts under which they are bound by a duty of confidentiality.

The school will not transfer your data to countries outside the European Economic Area.

How does the school protect data?

The school takes the security of your data seriously. The school has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by those parties listed in this policy in the performance of their duties.

Where the school engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the school keep data?

The retention periods for your personal data are as follows:

Employee Data	Statutory Retention Period
Payslips and general wages information	7 years
Working hours, name and address of employee, PPS numbers and statements of duties	7 years
Training records	7 years

Records relating to parental leave	8 years
Tax records	7 years
Records relating to workplace accidents	10 years
Employment permit records	7 years or duration of employment
CCTV recordings	28 days

See detailed Employee Records Retention Schedule for further details.

Your rights

As a data subject, you have a number of rights, these include:

- The right to have personal information processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- The right to be informed, this means that Loreto Wexford needs to tell you what data we are using, why we are using it and for what purpose as well as informing you of the details of any third parties in receipt of data from us;
- The right of access, you are allowed to see what data of yours we are processing if you request that from us;
- The right of rectification, that means if the data we are using is incorrect we must correct it;
- The right to erasure (or right to be forgotten), this means that you have the right to issue a request to us requesting the erasure of your personal data. However, in certain cases, under our obligations as an employer, we will have overriding legitimate grounds for continued processing and we may be unable to comply with such a request;
- The right to restrict processing, this means that you can ask you to stop using your data unless we have a legitimate lawful purpose for continuing to do so;
- The right to data portability, this means that you have the right to move your data to another controller and we must provide you with a copy of your data “in a structured, commonly used and machine-readable format”;
- The right to object, this means that you can object to the use of your data and we must stop using it unless we have an overriding legitimate reason to continue; and
- The right not to be subject to automated decision making, including profiling;
- The right to make a complaint; and
- The right to judicial remedy.

If you would like to exercise any of these rights, please contact the school’s Privacy Coordinator.

If you believe that the school has not complied with your data protection rights, you can complain to the Data Protection Commissioner by contacting:

Tel: 1890 25 22 31

Email: info@dataprotection.ie

Or you can download a “Raise a Concern” Form by going to:

https://www.dataprotection.ie/documents/gdpr_forms/Raise_a_Concern_with_Us_Form.pdf

What if you do not provide personal data?

You have some obligations under your employment contract to provide the school with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also

have to provide the school with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details and payment details, must be provided to enable the school to enter into a contract of employment with you. If you do not provide other information, this will hinder the school's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Your Data Protection Responsibilities

In every instance when you are working with another individual's personal data you must make sure to think at all times about the security of that data, this could be data belonging to another member of staff or data relating to a student or parent. It is advisable for staff to read the school's Privacy Policy so as to ensure that you follow certain guidelines relating to the security of personal data.

School guidelines include:

- Make sure to use strong passwords, for example a name is not sufficient, passwords should contain upper case and lower-case letters, numbers and special characters and be more than 8 characters in length;
- Screens should always be locked or computers shut down when classrooms are unattended;
- If for any reason you have to use a memory stick to transfer data, ensure that you purchase one that has one with encryption or a combination lock access system. The transfer of data may only be done on a direct instruction from management;
- School data should not be removed from the premises except under limited circumstances;
- Only store data on designated drives and only upload it to approved IT systems;
- Do not email data to your personal email account at any time;
- When paper files with personal data on them are not in use they should be stored away securely;
- Do not leave print outs with personal data in any areas where they may be visible to unauthorised personnel;
- Any hard copies of forms or documents with personal data on them that are not being retained and stored appropriately should be shredded and not disposed of in with regular waste; and
- Always keep information strictly confidential and do not disclose or discuss a student's or parent's personal information or circumstances with any unauthorised outside parties.

As well as

As well as adhering to the above guidelines, you are required to familiarise yourself with the Social Media Guidelines for staff regarding conduct on social media platforms. If you have not received a copy of these guidelines, please contact the principal.

General Data Protection queries should be addressed to the Data Protection Officer and they will then check out your query and come back to you.

Personal Data Breaches

Article 4(12) GDPR defines a 'personal data breach' as:

“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”.

The school may suffer a breach for a number of reasons including:

- the disclosure of confidential data to unauthorised individuals;
- improper disposal of documents;
- loss or theft of data or equipment on which data is kept;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of the school’s IT security;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- viruses or other security attacks on the school’s IT systems or networks;
- breaches of physical security;
- breach as a result of third party breach;
- confidential information left unlocked in accessible areas; and
- emails containing personal or sensitive information sent in error to the wrong recipient.

In the event of a breach of personal data occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence. If a staff member becomes aware of an actual, potential or suspected breach of personal data, he/she must report the incident to the Principal immediately.

No member of staff is permitted to take action themselves in the event of a breach, even if they have caused the breach themselves, only the specific staff are authorised to follow the school’s Personal Data Breach Procedure.

You have a responsibility to report all breaches, failure to do so may cause further disciplinary action.

Closed circuit monitoring

The school has closed circuit television cameras located at the front entrance and at the rear of the school. This is necessary in order to protect against theft or pilferage, for the security of students, staff and visitors, for the protection of school property and to prevent bullying. Access to the recorded material will be strictly limited to authorised personnel.

CCTV systems for surveillance purposes are installed according to local laws and regulations. Any person whose image has been recorded will be given the right to view a copy of the information recorded provided it has not be deleted.

The CCTV recordings are not used for staff monitoring.

Conclusion

At Loreto Wexford, we take the privacy of our staff seriously and we respect their rights and freedoms. Should any staff member be concerned about their rights, they should contact the school Principal or Data Protection Officer. The school reserves the right to update or amend this Policy at any time deemed appropriate to reflect any changes in our processing.