



OUR LADY'S SCHOOL
Data Protection Policy

Ratified by the Board of Management on:

Date: _____

Signature: _____

(Chair of the Board of Management)

Our Lady's School Data Protection Policy

MISSION STATEMENT

Our Lady's School is a community that embraces Christian values. The education it provides is rooted in a deep sense of faith.

We aim to create a positive inclusive environment which enables everyone to reach their full potential. We promote mutual respect within the school community and strive to provide a happy and secure atmosphere which fosters a love of learning.

We encourage the development of the whole person, by fostering the personal, spiritual and moral development of every student. The realisation of individual talents and academic excellence is paramount.

We aim to create a friendly, healthy, safe and caring environment which affirms our pride in the school.

We promote the development of the necessary skills so that students may become responsible members of society. It is our wish to see every student leave Our Lady's School with moral integrity and a heightened sense of social conscience.

Title

Data Protection Policy of Our Lady's School, Terenure.

Introductory Statement

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988-2018.

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Data Protection Principles

The school is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988-2018 which can be summarised as follows:

- **Obtain and process *Personal Data* fairly:** Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.
- **Keep it only for one or more specified and explicit lawful purposes:** The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.
- **Process it only in ways compatible with the purposes for which it was given initially:** Data relating to individuals will only be processed in a manner consistent with the purposes

for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

- **Keep *Personal Data* safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.
- **Keep *Personal Data* accurate, complete and up-to-date:** Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.
- **Ensure that it is adequate, relevant and not excessive:** Only the necessary amount of information required to provide an adequate service will be gathered and stored.
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given:** As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.
- **Provide a copy of their *personal data* to any individual, on request:** Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

Scope

Purpose of the Policy: The Data Protection Acts 1988-2018 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

In order to properly understand the school's obligations, there are some key terms which should be understood by all relevant school staff:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data means 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 i.e. the school.

Sensitive Personal Data refers to *Personal Data* regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the board of management, of Our Lady's School.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts 1988-2018.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the principal and board of management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

Safeguarding Against Data Protection and Security Risks

This policy helps to protect Our Lady's School from data security risks, including:

- **Breaches of security and confidentiality.** For instance, information being given out inappropriately.
- **Reputational damage.** For instance, the School could suffer if hackers successfully gained access to sensitive data.
- The risk of **large fines** or sanctions being imposed by the authorities.
- The **risks of being sued** for damages by individuals whose data has been mishandled

Other Legal Obligations

Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection. **For example:**

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to

the child's educational progress to the principal of another school to which a student is transferring

- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)
- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs")) such information as the Council may from time to time reasonably request
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to characteristic spirit of the School

Our Lady's School seeks to

- enable each student to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

Personal Data

The *Personal Data* records held by the school **may** include:

A. Staff records:

- (a) **Categories of staff data:** As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes:** Staff records are kept for the purposes of:

- the management and administration of school business (now and in the future)
- to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- to facilitate pension payments in the future
- human resources management
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies and for compliance with legislation relevant to the school.

(c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

B. Student records:

(a) **Categories of student data:** These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
 - name, address and contact details, PPS number
 - date and place of birth
 - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
 - religious belief
 - racial or ethnic origin
 - membership of the Traveller community, where relevant
 - whether they (or their parents) are medical card holders
 - whether English is the student's first language and/or whether the student requires English language support
 - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements). See the template "Guidance on Taking and Using Images of Children in Schools"
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish

- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes:** The purposes for keeping student records are:

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's "Guidance for Taking and Using Images of Pupils in Schools" (see template)
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirements for their course,
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

(c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

C. Board of management records:

(a) **Categories** of board of management data: These may include:

- Name, address and contact details of each member of the board of management (including former members of the board of management)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.

(b) **Purposes:** To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

(c) **Location:** In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access.

D. Other records:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors

- (a) **Categories of data:** the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
 - address
 - contact details
 - PPS number
 - tax details
 - bank details and
 - amount paid.
- (b) **Purposes:** This information is required 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.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Charity tax-back forms

- (a) **Categories of data:** the school may hold the following data in relation to donors who have made charitable donations to the school:
- name
 - address
 - telephone number
 - PPS number
 - tax rate
 - signature and
 - the gross amount of the donation.
- (b) **Purposes:** Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents' name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

CCTV images/recordings

- (a) **Categories:** CCTV is installed in some schools, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.
- (b) **Purposes:** Safety and security of staff, students and visitors and to safeguard school property and equipment.
- (c) **Location:** Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in the Principal's office.

- (d) **Security:** Access to images/recordings is restricted to the Senior Management Team i.e. the principal & deputy principal of the school. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988-2018.

Examination results

- (a) **Categories:** The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock-examinations results.
- (b) **Purposes:** The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

October Returns

- (a) **Categories:** At the beginning of each academic year (and for 1st year or transferring students, on enrolment) parents/guardians and students are asked to provide the school with certain information so that the School can make returns to the Department of Education and Skills ("DES") referred to as "October Returns". These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The October Return contains individualised data (such as an individual student's PPS number) which acts as an "identifier" for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section).
- (b) **Purposes:** The school asks parents/guardians and students to complete October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school. The main purpose of the October Returns is for the DES to determine whether the student qualifies for English language support and/or additional resources and support to meet their particular educational needs. The October Returns are submitted to the DES electronically. The DES has their own policy governing the security of the data sent to them by all post-primary schools. The co-operation of each student and/or their parents/guardians in completing the October Return is greatly appreciated as the school's aim is to ensure that each student is assisted in every way to ensure that s/he meets his/her full potential.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Responsibilities and Compliance

Everyone who works for or with Our Lady's School has responsibility for ensuring data is collected, stored, and handled appropriately. Each person who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Specific responsibilities are outlined in more detail below.

The Principal as Data Protection Officer (DPO) will

- ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff induction, staff meetings and via the staff handbook.
- ensure that there are regular updates to data protection awareness, so that data protection is a "living" process aligned to the school's ethos
- periodically check data held regarding accuracy

The Board of Management as Data Controller will:

- inform the person or persons involved, that a breach of confidentiality has occurred and that their personal data may have been compromised.
- investigate where a breach of security has occurred and invoke appropriate action
- review and update the Data Protection Policy if required.
- ensure that only relevant data is processed
- check to see if clerical and computer procedures are adequate to ensure accuracy.
- reassure parents/guardians that the Data Protection Policy has been reviewed
- in tandem with the DPO, advise and inform employees of the need to work within the demands of the school's Data Protection policy.

Our Lady's School Staff as Data Processors will:

- be required to sign off to confirm they have read and understand the Data Protection Policy and Procedures.
- check that any information that they provide in connection with their employment is accurate and up to date.
- notify the school of any changes to information they have provided, for example change of address.
- ensure that personal information relating to students or their families is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.

Sanctions and Disciplinary Action

Given the serious consequences that may arise, Our Lady's School may invoke appropriate disciplinary procedures for failure to adhere to the school's policy on Data Protection

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Compliance Monitoring and Review

Our Lady's School will undertake regular reviews of internal procedures and changes in the legislation to ensure ongoing compliance with General Data Protection Regulation. This will include an annual review.

Data Security

Overview

- Access to data will be restricted to authorised staff on a "need-to-know" basis and where it is needed to fulfil their duties and responsibilities.
- Data will not be shared informally.
- Our Lady's School will provide training to all staff to help them understand their responsibilities when processing data.
- Staff will keep all data secure by taking sensible precautions and following the guidelines below.
- Strong passwords will be used, and never shared.
- Personal data will not be disclosed to unauthorised people, either within Our Lady's School or externally.
- Data will be regularly reviewed and if found to be out of date, will be deleted or disposed of according to the guidelines below.
- Staff will request help from the DPO or Data Controller if they are unsure about any aspect of data protection.

Data Storage

The security of personal information relating to students and staff is a very important consideration under the Data Protection Acts and is taken very seriously at Our Lady's School. Appropriate security measures will be taken by the school to protect unauthorised access to this data and to the data it is collecting and storing on behalf of the Department of Education and Skills (DES).

A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised staff on a "need-to-know" basis.
- Manual files will be stored in a relevant filing system, located away from public areas.
- Computerised data will be held under password protected files.
- Any information which needs to be disposed of will be done so carefully and thoroughly.
- The premises at Our Lady's School are protected by monitored CCTV cameras.

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it. This also applies to data that is usually stored electronically but has been printed out for a valid reason:

- When not required, the paper or files will be kept in a relevant filing system
- All personnel will ensure that personal data, paper and printouts are not left where unauthorised people could see them.
- Data will be shredded and disposed of securely when no longer required.

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (e.g. a USB key), these will be kept locked away (and ideally encrypted) when not being used.
- Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location.
- Data will be backed up frequently.
- All servers and computers containing data will be protected by an approved security software and a firewall.

Data Use

Personal data is at often at the greatest risk of loss, corruption, or theft when it is being used or accessed:

To mitigate this risk :-

- when working with personal data, all personnel will ensure that the screens of their computers/tablets/apps are always locked when left unattended.
- personal data shared by email will be downloaded, stored securely, and then deleted.
- data will be encrypted before being transferred electronically where appropriate.
- staff will not save copies of personal data to their own computers.

Data Accuracy

Our Lady's School is cognisant of its duty to take reasonable steps to ensure that data is kept accurate and up-to-date.

- Data will be held in as few places as necessary.
- Every opportunity will be taken to ensure that data is updated (for example, by updating a student's contact information).
- Our Lady's School will make it as easy as possible for data subjects to update the information held about them, over the phone, or by email.
- Data will be updated as and when inaccuracies are discovered (for example), if a data subject can no longer be reached on their stored telephone number, it will be removed from the database.

Data Disclosure to Third Parties

As the Data Controller, the Board of Management is responsible for any personal data passed to third parties and care will be given to procedures and security.

The only data disclosed to third parties in the normal course of events is as described in Our Lady's School's Privacy Notices and Register of Personal Data Records.

The following list includes examples of such organisations but is not exhaustive:

- An Garda Síochána
- TúsIa
- Department of Education and Skills
- Insurance Company
- Health and Safety Authority
- Workplace Relations Commission
- Revenue Commissioners

Note: Data Collected Through Garda Vetting

Our Lady's School understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns, the information will be dealt with on a confidential basis. All information pertaining to such a situation will be stored in the same way as other data. The Board of Management will not pass on a copy of a Garda Vetting Form to any other party.

Data Erasure and Disposal

When documentation or computer files containing personal data are no longer required, the information will be disposed of carefully to continue to ensure the confidentiality of the data.

Paper-based files and information no longer required, will be safely disposed of in shredding receptacles. Usually the data will be shredded on site by school personnel – but occasionally a third party data destruction specialist will be employed and vetted staff will collect documents which will be shredded on site by the specialists.

In the case of personal information held electronically, temporary files containing personal information will be reviewed regularly and deleted when no longer required.

When personal data reaches the point where the retention period has expired, the information will also be securely deleted and removed. In the event that IT equipment containing personal data is no longer required, all data stored on the devices will be removed prior to disposal.

Links to other policies and to curriculum delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Mobile Phone Code
- Admissions/Enrolment Policy
- CCTV Policy
- ICT Acceptable Usage Policy

Processing in line with data subject's rights

Data in this school will be processed in line with the data subjects' rights.

Data subjects have a right to:

- (a) Request access to any data held about them by a data controller
- (b) Prevent the processing of their data for direct-marketing purposes
- (c) Ask to have inaccurate data amended
- (d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with a data access requests

Section 3 access request

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request

Individuals are entitled to a copy of their personal data on written request.

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within 30 days
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Subject Access Request (SAR) Handling Procedure

The Data Protection Acts 1988-2018 provide for a right of access by an individual data subject to personal information held by Our Lady's School. A person seeking information, the Data Subject, is required to familiarise himself/herself with this policy. 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 supplied that relates to another individual. Although from time to time an individual may request by telephone details of some elements of their personal data, formal SARs must be submitted in writing, either electronically or by post.

Students making access requests

The Board of Management of Our Lady's School, in compliance with the GDPR recognises that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned, and also their rights in relation to the processing of personal data. It aims to balance the complementary rights of the child outlined in Articles 16(i) and 5 of the UN Convention of the Rights of the Child, these being that "no child shall be subjected to arbitrary or unlawful interference with his and her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour" and "rights and duties of parents to provide..... in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognised in the present Convention".

- 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 under the age of eighteen 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.
- Each student request for Access to Personal Data will be assessed individually.

Parents making access requests on behalf of their son/daughter

Where a parent/guardian makes an access request on behalf of his/her son/daughter (a student aged 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 son/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 subject to the provisions above.

Others making an access request

The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of the processing of their personal data. Under the GDPR and the current Data Protection Acts (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- the reasons why their data is being processed,
- the description of the personal data concerning them,
- anyone who has received or will receive their personal data, and
- details of the origin of their data if it was not collected from them.

To ensure SARs are responded to in a timely and effective manner, responsibility for identification and management of all requests will be assigned to a Designated Person. At Our Lady's School the Designated Person is the Principal and in her prolonged absence, the Deputy Principal.

Steps in Making a Subject Access Request (SAR)

- The Data Subject applies in writing requesting access to his/her data. The school reserves the right to request official proof of identity (e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification
- On receipt of the Data Access Request, the Principal will check the validity of the access request and check that sufficient information to locate the data requested has been supplied. It may be necessary for the Principal to contact the data subject in the event that further details are required with a view to processing the access request.
- The Principal will log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.
- The Principal will ensure that all relevant manual files and computers are checked for the data in respect of which the access request is made.
- The Principal will ensure that the information is supplied promptly and within one month of first receiving the request.
- If data relating to a Third Party is involved, it will not be disclosed without the consent of that Third party or alternatively the data will be anonymised in order to conceal the identity of the third party. Where it is not possible to anonymise or conceal the identity of the third party the data to ensure that the Third Party is not identified, then that item of data may not be released.
- Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.
- The Principal will ensure that the information is provided in an intelligible form (e.g. codes explained) where possible.
- The documents supplied will be numbered where appropriate.
- The Principal will sign off on the data supplied.
- The school reserves the right to supply personal information to an individual in an electronic format e.g. on USB etc.
- Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

Appealing a Decision in Relation to a Data Access Request

The Board of Management of Our Lady's School is respectful of the right of the Data Subject to appeal a decision made in relation to a request for data from this school. To appeal a decision, the Data Subject is advised to write to or email the Data Protection Commissioner explaining the case:-

Canal House, Station Road, Portarlington, Co. Laois
info@dataprotection.ie

The correspondence should include

- the name of this school
- the steps taken to have concerns dealt with
- details of all emails, phone calls, letters between the Data Subject and this school.

Data Breaches

Definition: A data breach is an incident in which personal data has been lost, accessed, and/or disclosed in an unauthorised fashion.

This would include, for instance, loss or theft of a laptop containing staff or student details, an email with personal information being sent to the wrong recipient, as well as more organised incidents of external hacking.

All school personnel have a responsibility to take immediate action if there is a data breach.

- If a staff member suspects at any time and for any reason that a breach may have occurred, then there is a need to report it to the DPO/Data Controller as an urgent priority
- Once notification of an actual or suspected breach has been received, the DPO/Data Controller will put the Data Breach Procedure into operation with immediate effect.

Data Breach Handling Procedure

The purpose of the Data Breach Procedure here below, is to ensure that all necessary steps are taken to:

- (i) contain the breach and prevent further loss of data
- (ii) ensure data subjects affected are advised (where necessary)
- (iii) comply with the law on reporting the incident to the Data Protection Commissioner if necessary
- (iv) learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future

Data Breach Response Plan

- A Breach Incident Leader will be nominated. This will typically be the DPO.
- Stakeholders will be identified
- A breach response handling team will be formed - comprising the school's Senior Management Team / the IT Coordinator / external IT supplier etc.
- The five-step process below will be initiated, with an evaluation after each stage

The information communicated to data subjects will include information on the nature of the personal data breach and a contact point where more information can be obtained. It will recommend measures to mitigate the possible adverse effects of the personal data breach.

The maximum timeframe for notification to the Office of the Data Protection Commissioner has been set at 72 hours from the time the incident is first discovered.

Providing information over the phone

In our school, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Implementation arrangements, roles and responsibilities

In our school the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of management:	Data Controller
Principal:	Implementation of Policy. Data Protection Officer.
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Ratification & communication

When the Data Protection Policy has been ratified by the Board of Management, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the

school community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Enrolment Pack, by either enclosing it or incorporating it as an appendix to the enrolment form.

Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the principal and a sub-committee of the board of management.

At least one annual report should be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and evaluating the policy

The policy should be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills), legislation and feedback from parents/guardians, students, school staff and others. The policy should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Signed:

For and behalf of board of management

Date: