Jesus and Mary College Our Lady's Grove

GDPR Data Protection Policy

2018

Table of Contents

GDPR Data Protection Policy

Mission Statement

Jesus and Mary College, Our Lady's Grove is a Catholic Community in keeping with the educational philosophy of St. Claudine Thevenet and the stated ethos of the school. We are committed to providing a quality education in pursuit of excellence. We endeavour to provide a teaching and learning environment which encourages the school community to develop to its full potential cognisant of all its talents and skills. We aim to work together in a safe, respectful, caring and just environment. We value the principles of mutual respect, equality and tolerance encouraging positive self-image, confidence and pride in all achievements.

Rationale

The school's GDPR Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988, 2003 and GDPR 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. 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. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation.

It should be remembered that information pertaining to criminal activity will be provided to appropriate authorities to ensure the safety and welfare of our community in accordance with the relevant sections of the Acts.

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.

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.

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.

➢ 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 and 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 educational 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 or immunization administration.

➢ Under Children First: National Guidance for the Protection and Welfare of Children (2017), 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) and to maintain documentation according to the highest confidentiality standards.

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
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- physical or mental health condition
- sexual orientation
- 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 Grove. The principal, with the support of the secretary and other relevant staff members manage the data. The principal, on behalf of the Board of Management, is the data protection officer, acting as the point of contact for any data management queries. A data processor

processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data during the course of his or her employment.

Data Protection Principles

Jesus and Mary College, Our Lady's Grove 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 GDPR.

The GDPR identifies children as vulnerable persons deserving of specific protection. Children under the age of consent can never themselves give consent to the processing of their personal data.

Individual rights under GDPR include:

- Staff members, prospective staff members and parents/guardians of students have **The right to be informed** as to why personal data is being collected and how it is to be used, shared and stored.
- **The right to access** – This policy provides clear processes for how data subjects may obtain confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the school shall provide a copy of the personal data, free of charge, in an electronic format.
- **The right to rectification** – Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the school discloses personal data to third parties, which is limited solely to the Department of Education and Skills, the National Council for Special Education and professional services such as therapists and psychologist as required and only after signed consent from parents, the school must inform them of the rectification where possible.
- **The right to be forgotten** – Also known as data erasure, the conditions for erasure include the data no longer being relevant to original purposes for processing or a data subject withdrawing consent. It should also be noted that this right requires the school to compare the subjects' rights to the public interest in the availability of the data when considering such requests. If an individual contacts the school and requests that their data be removed from its databases, it will be obliged to do so, unless it has a legitimate reason to retain the data.
- **The right to restrict processing** – In some situations, this right gives an individual an alternative to requiring data to be erased; in others, it allows the individual to require data to be held whilst other challenges are resolved. If personal data are 'restricted', then the school may only store the data. It may not further process the data unless the individual consents or the processing is necessary for establishment of legal claims, for the protection of the rights of another natural or legal person or for reasons of important public interest.
- **The right to data portability** – Data subjects may receive the personal data concerning them, which they have previously provided and have the right to transmit that data to another controller such as another school.
- **The right to compensation & liability data** – Subjects can sue both controllers and processors for compensation for pecuniary or nonpecuniary damage (e.g. damages for distress) suffered as a result of a breach of the GDPR.

WE at Our Lady's Grove commit to the following *practical guidelines*.
We will:

- **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 terms of GDPR Policy. The information will be obtained and processed fairly.
- **Privacy by design**: The school will only collect data absolutely necessary for the completion of its duties (data minimisation). Access to personal data will be limited to

those needing to act out the data processing. Before any protocols of this policy are changed, a Data Protection Impact Assessment (DPIA) shall be conducted where a type of processing is likely to result in a high risk to the individual data subjects.

- **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 of a manual nature is securely stored under lock and key. Electronically stored data is password protected. Certain staff members dealing with sensitive data have been supplied with a USB key which is encrypted and utilized to store sensitive information on that device. Passwords are periodically changed to improve security. 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 staff member however records must not be altered or destroyed without proper authorisation. If alteration/correction is required, 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.

Personal Data

The school uses a Web based administration software which is held on a server off site. *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)
- facilitating the payment of staff, calculating other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- facilitating pension payments in the future
- human resources management
- recording promotions made (documentation relating to applications for promotions) and changes in responsibilities etc.
- enabling 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)
- enabling 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
- 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.

(d) **Security:** Sensitive manual records are kept within a secure relevant filing system, management information system records will be protected by account permissions, and passwords which ensure information is only available to relevant personnel. Certain information is subject to encryption. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

(e) **Retention Protocols:**

Staff Recruitment Records	Retention Timeframe	Final Disposition
Applications & CVs of candidates called for interview but were unsuccessful	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Candidates shortlisted but unsuccessful at Interview		
Candidates shortlisted and are successful but do not accept offer		
Interview board marking scheme & board Notes		
Panel recommendation by interview board		
Database of applications		Confidential shredding and/or deletion database
Selection criteria		
Applications of candidates not shortlisted		Deletion of associated email account
Unsolicited applications for jobs (typically for incidental subbing)	12 months from receipt of application	Confidential shredding

Staff Personnel Files	Retention Timeframe	Final Disposition
Carer's leave	Retain for 2 years following retirement or resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school).	Confidential shredding
Working Time Act (attendance hours, holidays, breaks)	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).	
Allegations/complaints	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served).	
Grievance and disciplinary records		

Occupational Health Records	Final Disposition	Retention Timeframe
Sickness absence records/certificates	Confidential shredding or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Pre-employment medical assessment		
Occupational health referral		
Correspondence re retirement on ill-health grounds		
Accident/injury at work reports		Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy).
Sick leave records (sick benefit forms)	Confidential shredding	In case of audit/refunds, current year plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Superannuation /Pension /Retirement records	Final Disposition	Comments
Records of previous service (incl. correspondence with previous employers)	N/A	Indefinitely
Pension calculation	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school).
Pension increases		
Salary claim forms		

Promotion process for posts of responsibility	Final Disposition	Comments
Calculation of service	N/A	Retain indefinitely on master file
Promotions/POR Board master files		Retain indefinitely on master file
Promotions/POR Boards assessment report files		Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents		Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.
Correspondence from candidates re feedback		Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.

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
- 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/ETB which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Parents will be advised if a particular incident is 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 the contacting of parents/guardians 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 policy
- 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.

(d) **Security**: Manual records are kept in secure filing cabinets. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

Some documents may be temporarily written and stored by staff members in their classrooms. Anything of a confidential nature is stored securely. Digital Information is held by the Management Information System VSWare. VSware uses the highest levels of encryption. It has systems to prevent unauthorized access including automatically logging out after a fixed period. Staff members use a username and password to access the system and should adhere to and be aware of the following:

• Users are allocated different access rights to VSware. The access rights are solely determined by the school. At present, the Principal and Deputy Principal are given full administrator rights.

• The secretary is also an administrator but is not given access to information regarding academic progress. Mainstream teachers are given general access for their class only and are not granted administrative rights.

• A unique username and password is provided to each user. Users should keep their username and password confidential and not disclose it to anybody or allow any person to access the system using their username and password. Staff members should change their passwords every 6 months and never store the passwords on any computers.

• VSware should only be used for the purposes of managing internal school administration activities and for no other purpose. VSware should not be accessed in the event of suspension or termination of the users' position at the school.

• The school is responsible for ensuring that access to the VSware system for terminated or suspended users is disabled.

• Each user should ensure they are familiar with the VSware before use. All queries should be referred to the Deputy Principal.

• The user should notify the Deputy Principal in the event of any misuse or loss of their username and password.

• The user should only login to the VSware when in a secure and non-public environment, e.g. the school or home of the user.
• The user should sign out of VSware when leaving the device unattended.
• VSware should not be used to deal with emergency situations and it should not be relied upon during such times. Therefore, paper copies of emergency contact details are stored and locked in the secretary's desk.
• VSware should not be accessed through an unsecure network or internet connection.

Student Records	Retention	Final disposition
Registers/Roll books	Indefinitely. Archive when class leaves + 2 years	N/A
Disciplinary notes	Never destroy	N/A
Records of school tours/trips, including permission slips	Never destroy	N/A
Enrolment forms	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Student transfer documentation		
End-of-term/year reports		
Results of in-school tests, including standardised test results	Actual test papers retained for one year. Results retained until a pupil is 18 (age of majority) plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served).	

Sensitive Personal Data Students	Retention	Final disposition
Psychological assessments and other professional reports	Never destroy	N/A
Special education needs files including reviews, correspondence and Individual Education Plans		
Accident reports		
Child protection records		
Section 29 appeal records	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Enrolment/transfer forms where child is not enrolled or refused enrolment		
Records of complaints made by parents/ guardians	Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy. If it is a complaint of a more mundane nature or other minor matter, then only until the student reaches 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)	Confidential shredding or N/A, depending on the nature of the records.

D Creditors/Debtors

Categories of Creditors/Debtors Data: These may include

- name
- address
- contact details
- PPS number
- tax details
- bank details
- amount paid
- amount owed

The rationale for seeking and retaining a creditor's/debtor's personal data is as follows:

- 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.

E *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.

(d) **Security:** These records are kept both in manual format (personal file within a *relevant filing system*), computer record (database) or both. Information is kept locked and password protected. USB keys are encrypted. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

F *Child Safeguarding Information*

(a) **Categories**: Codified and redacted data relating to Child Safeguarding concerns. This would include both those that are reported to TUSLA and those that were not but might be into the future. Files may be added or taken away from this level of security over time depending on the evolving context of the individual concern or issue.

(b) **Purposes**: To keep a written record of possible or actual child safeguarding concerns both for reporting to TUSLA, for oversight reporting to the Board of Management and for legal retention as per the Child Safeguarding legislation.

(c) **Location**: Codified and redacted school files are kept in a locked safe in a strong room. TUSLA documentation is kept in a separate safe in a strong room. These are accessible only by the DLP.

(d) **Security**: Access to these files is restricted by a strong room lock and password protected safes. Access is limited to the DLP. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

G *CCTV images/recordings*

(a) **Categories**: CCTV is installed both inside and outside the school, as detailed in the CCTV Policy. The CCTV system 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 an administration office within the school.

(d) **Security**: Access to images/recordings is restricted to authorised personnel. Tapes, DVDs, hard disk recordings are retained for 14 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 and 2003 and GDPR 2018. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

H 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. Examination results are also stored digitally on VSWare. (Please see page 9).

(c) Security: The format in which these records are kept are both manual (personal file within a *relevant filing system*) and computer records (database).Information is stored securely and password protected in the case of database. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

I *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 for information to allow the completion of 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 she meets 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.

(d) **Security**: These records are kept both manually (securely stored with restricted access) and on a database which is password protected. Data is only held in locked and code protected offices. The facility is protected by a monitored security system when not in use.

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
- Guidance Policy
- Mobile Phone Policy
- Admissions Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/CSPE etc.

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 40 days
- Fee may apply but cannot exceed €6.35
- 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.

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 in circumstances where the identity of the caller cannot be verified
- Normally personal information is not provided over the phone and phone requests for students to leave school are discouraged as the caller cannot be identified (please see our Attendance Policy)

RIGHT OF ACCESS Article 15 GDPR

Under Article 15 of the GDPR, data subjects have a right to obtain a copy, of any information relating to them kept on computer or in a structured manual filing system or intended for such a system by the school. All they need to do is write to the organisation and request, under the GDPR, a copy of the personal data it holds in relation to them.

Requests should read as follows:

Dear Data Protection Officer, Our Lady's Grove
...
I wish to make an access request under Article 15 of the General Data Protection Regulation (GDPR) for a copy of any information you keep about me, on computer or in manual form in relation to...
(**Please be as specific as possible in relation to the personal data you wish to access).**

Data subjects must provide evidence of their identity. This is to make sure that personal information is not given to the wrong person.

We will respond to access requests within one month of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). If we need to extend the period for replying to your request, we will inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.
There is no fee payable by you to make an access request. However, where the organisation believes a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the organisation may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s). The burden of demonstrating why a request is manifestly unfounded or excessive rests on the organisation.

Exceptions to the right of access

The Data Protection Act 2018 sets out some limited circumstances in which Our Lady's Grove may not be required to provide you with a copy of your personal data.

- to safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the State
- for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
- for the administration of any tax, duty or other money due or owing to the State or a local authority.
- in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure
- for the enforcement of civil law claims, including matters relating to any liability of an organisation in respect of damages, compensation or other liabilities or debts related to the claim, or
- For the purposes of estimating the amount of the liability of an organisation on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the interests of the organisation in relation to the claim.

In addition, Our Lady's Grove may not provide a data subject with a copy of their personal data where the data consists of an expression of opinion about them by another person given in confidence, or on the understanding that it would be treated as confidential, to a person who has a legitimate interest in receiving the information.
The data subject's right of access may also be restricted where, in the opinion of a medical professional, to grant access to the data would be likely to cause serious harm to the individual's physical or mental health. Access to personal data kept for, or obtained in the course of, carrying out of social work by a public authority, public body, voluntary organisation or other body may be similarly restricted[2].

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 members 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:	Data Protection Officer/Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Responsibilities and Compliance

Everyone who works for or with Jesus and Mary College, Our Lady's Grove 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 Grove 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 Grove 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 Grove 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.

Signed: …….

For and behalf of board of management

Date: ……