OUR LADY OF MERCY SECONDARY SCHOOL

DATA PROTECTION POLICY

1. Purpose and Scope

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

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

1.3 The Irish *Data Protection Act (2018)* and the European *General Data Protection Regulation (2016)* are the primary legislative sources.[1] As such they impose statutory responsibilities on the school as well as providing a number of fundamental rights (for members and others) in relation to personal data.

1.4 The school recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. Relevant policies and procedures apply to all school members and others (including prospective or potential members within the school).

1.5 Any amendments to this Data Protection Policy will be communicated through the school website and other appropriate channels, including direct communication with data subjects where this is appropriate. We will endeavour to notify you if at any time we propose to use Personal Data in a manner that is significantly different to that stated in our Policy, or, was otherwise communicated to you at the time that it was collected.

1.6 The school is a *data controller* of *personal data* relating to its past, present and future members and other members of the school community. Formally, the statutory responsibility of Controller is assigned to the school's Board of Management. The Principal is assigned the role of co-ordinating the implementation of this Policy and for ensuring that all staff who handle or have access to Personal Data are familiar with their responsibilities.

[1] The school is also cognisant of other legislation which relates to the processing of personal data, whether in manual or in electronic form. For example, the 2011 e-Privacy Regulations (S.I. No. 336 of 2011) provide statutory guidance with regard to certain data processing operations (e.g. direct marketing, cookie notifications on the school's website etc.).

Name	Responsibility
School Board of Management	Data Controller
GDPR Officer (Principal)	Implementation of Policy
All members	Adherence to the Data Processing Principles
Entire school Community	Awareness and Respect for all Personal Data

2.1 **Processing** is the term used to describe any task that is carried out with personal data e.g. collection, recording, structuring, alteration, retrieval, consultation, erasure as well as disclosure by transmission, dissemination or otherwise making available. Processing can include any activity that might relate to personal data under the control of the school, including the storage of personal data, regardless of whether the records are processed by automated or manual means.

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

2.3 These principles, set out under GDPR, establish a statutory requirement that personal data must be:

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

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

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

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

(v) kept for no longer than is necessary for the purposes for which the personal data are processed[2]; (**storage limitation**);

[2] Data may be stored for longer periods if being processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (subject to appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject).

(vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

2.4 GDPR also establishes **Accountability** as a core data processing principle. This places a statutory responsibility on the school, as Data Controller, to be able to demonstrate compliance with the other principles i.e. the 6 data processing principles set out in the previous paragraph (2.3 above).

3.1 Whenever the school is processing personal data, all of the principles listed in the previous section(s), must be obeyed. In addition, at least one of the following bases (GDPR Article 6) must apply if the processing is to be lawful,

(i) compliance with a legal obligation

(ii) necessity in the public interest

(iii) legitimate interests of the controller

(iv) contract

(v) consent

(vi) vital interests of the data subject.

3.2 When processing **special category personal data**, the school will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9.[3] Special categories of personal data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.1 **Record of Processing Activities** This policy sets out the purposes for which the school collects and uses personal data for each of the various categories of data held.

[3] GDPR Article 9 sets out the lawful bases that apply to the processing of special categories of personal data.

4.2 **Members' Records** The purposes for processing members' personal data include the following: [4]

(i) to provide information prior to application

(ii) to determine whether an applicant satisfies the school's admission criteria;

(iii) to ensure that members benefit from relevant additional supports;

(iv) to contact members in case of emergency;

(v) to monitor communication and to provide a sound basis for advising members;

(vi) to communicate information about, and record participation in, school events etc.;

(vii) to compile posts, establish a school website, and to keep a record of the history of the school;

(viii) to comply with legislative or administrative requirements;

(ix) to furnish documentation/ information about the member to the Department of Education and Skills, an Garda Síochána, TUSLA and others in compliance with relevant laws and direction.

4.3 **School Board of Management Records** Board of Management records are kept in accordance with the policies of the school. Minutes of Board of Management meetings record attendance, items discussed, and decisions taken. Board of Management business is considered confidential to the members of the Board of Management

4.4 **Financial Records** This information is required for routine management and administration of the school's financial affairs, including the payment of fees, invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

5.1 **Recipients** These are defined as organisations and individuals to whom the school transfers or discloses personal data. Recipients may be data controllers, joint controllers or processors. A list of the categories of recipients used by the school is provided in the appendices (Appendix 3). This list may be subject to change from time to time.

[4] Appendix 2 sets out the type of personal data being processed by the school and the purposes for which this data is being processed. This list is likely to be subject to revision from time to time. For example, changes in legislation may require adjustments in the personal data processing.

5.2 **Data Sharing Guidelines**

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

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

(iii) Most data transfer to other bodies arises as a consequence of legal obligations that are on the school, and the majority of the data recipients are Controllers in their own right, for example, the Department of Education and Skills. As such their actions will be governed by national and European data protection legislation as well their own organisational policies.[5]

(iv) Some of the school's operations require support from specialist service providers. For example, the school may use remote IT back-up and restore services to maintain data security and integrity. In cases such as these, where we use specialist data processors, we will ensure that the appropriate security guarantees have been provided and that there is a signed processing agreement in place.

6.1 **Definition of a Personal Data Breach** A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6.2 **Consequences of a Data Breach**

(i) A breach can have a significant adverse effect on individuals, which can result in physical, material or non-material damage. This can include discrimination, identity

[5] The Data Protection Policy of the Department of Education can be viewed on its website.

theft or fraud, financial loss, damage to reputation, loss of confidentiality etc. Children because of their age may be particularly impacted.

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

(iii) It should be noted the consequences of a data breach could include disciplinary action, criminal prosecution and financial penalties or damages for the school and participating individuals.[6]

6.3 **Responding to a Data Breach**

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

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

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

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

7.1 **Your Rights** Personal Data will be processed by the school in a manner that is respectful of the rights of data subjects. Under GDPR these include[7]

(i) the right to information

(ii) the right of access

(iii) the right to rectification

[6] The Data Protection Act 2018 established a number of offences whereby breaches of the Act can result in fines and/or imprisonment.

[7] For further information on your rights see www.GDPRandYOU.ie.

(iv) the right to erasure ("right to be forgotten")

(v) the right to restrict processing

(vi) the right to data portability

(vii) the right to object

(viii) the right not to be subject to automated decision making

(ix) the right to withdraw consent

(x) the right to complain.

7.2 **Right to be Informed** You are entitled to information about how your personal data will be processed. We address this right primarily through the publication of this Data Protection Policy. We also publish additional privacy notices/statements which we provide at specific data collection times, for example, our Website Data Privacy Statement is available to all users of our website. Should you seek further clarification, or information that is not explicit in our Policy or Privacy Statements, then you are requested to forward your query to the school.

7.3 **Right of Access** You are entitled to see any information we hold about you. The school will, on receipt of a request from a data subject, confirm whether or not their personal data is being processed. In addition, a data subject can request a copy of their personal data. The school in responding to a right of access must ensure that it does not adversely affect the rights of others.

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

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

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

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

7.8 **Right to object** Data subjects have the right to object when processing is based on the school's legitimate interests or relates to a task carried out in the public interest (e.g. the

processing of special categories of personal data may rely on the school's legitimate interest in disassociation with a member's political affiliation). The school must demonstrate compelling legitimate grounds if such processing is to continue.

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

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

7.11 **Limitations on Rights** While the school will always facilitate the exercise of your rights, it is recognised that they are not unconditional: the school may need to give consideration to other obligations.[8]

7.12 **Right to Complain**

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

(ii) A matter that is still unresolved may then be referred to the school's Data Controller (i.e., the Board of Management) by writing to the Secretary to the Board of Management, Our Lady of Mercy Secondary School, Mourne Road, Drimnagh, D12 HT22.

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

Telephone	+353 57 8684800
	+353 (0)761 104 800
Lo Call Number	1890 252 231
Fax	+353 57 868 4757
E-mail	info@dataprotection.ie
Post	Data Protection Commission
	Canal House, Station Road
	Portarlington, Co. Laois

[8] See GDPR Articles 12-23 for a full explanation of subject rights and their application.

R32 AP23

Website www.dataprotection.ie

Appendix 1: Glossary

Controller or **Data Controller** - an entity or person who, alone or jointly with others, determines the purposes and means of the processing of personal data. In this policy, the data controller is the Board of Management.

Consent - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Commission - the national supervisory authority responsible for monitoring the enforcing the data protection legislation within Ireland. The DPC is the organisation to which SCHOOLs as data controllers must notify data breaches where there is risk involved.

Data Protection Legislation – this includes (i) the General Data Protection Regulation (GDPR) - *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and (ii) the Irish Data Protection Act (2018). GDPR is set out in 99 separate *Articles*, each of which provides a statement of the actual law. The regulation also includes 171 Recitals to provide explanatory commentary.

Data Subject - a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

Data concerning health - personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. This is an example of special category data (as is data concerning special education needs).

Personal data - any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor or **Data Processor** - a person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract.

Profiling - any form of automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

(Relevant) Filing System - any set of information that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Special categories of data - personal data revealing racial or ethnic origin, political opinions,

religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Appendix 2: Personal Data and related Processing Purposes

PURPOSES FOR PROCESSING	DESCRIPTION OF PERSONAL DATA
1. Contact and identification information This information is needed to identify, contact and enrol students.	
Purposes may include: • to add names to a contact list prior to formal application • to provide appropriate information to prospective members • to make contact in case of emergency (e.g. death, accident) • to send SMS text messages, WhatsApp, and emails about meetings, etc.	Information required to confirm member identity and contact through communications: • Member name • Date of birth • Contact details (to include phone numbers, email addresses etc).
2. Application information We use this to determine whether an applicant meets eligibility requirements.	
In addition to data outlined at (1) above, we collect personal data.	Information as required to ascertain eligibility:
Where the member is offered a place, contact information spreadsheet is updated. Use of photographs for general communication, social media, website etc.: Photographs, and recorded images of members may be taken at events and to celebrate events, compile communications, establish a website, record events, and to keep a record of the history of the school.	• Name and address • Details of service, etc. • Copy of any reports necessary (Primary school, NEPS etc.) • Consent to use (for these purposes) images or recordings in printed or digital format. • Separate consents will be sought for different publication forums.
3. Personal data gathered during member's time in the SCHOOL We cannot meet our statutory obligation to deliver appropriate education to students and/or we cannot satisfy our duty of care to each student without processing this information.	
Internal processes: This information (e.g. disciplinary process) is required to meet the school's duty of care to all its members, to comply with legal obligations and to run the school safely and effectively. Data collected in these processes may be transferred to the school's insurer and/or legal advisors or management body (JMB) as appropriate where required for disputes resolution, fact verification, and for litigation purposes.	• Records of complaints. • Records relating to internal processes (disciplinary etc.) including any written data and records.
Accident and injury reports: This information is processed to operate a safe environment for members, to identify and mitigate any potential risks, and to report incidents/accidents. This data may be transferred to the school's insurance company and/or indemnifying body and/or legal advisors as appropriate. Data will be shared with An Garda Síochána and the Health & Safety Authority where appropriate.	• Accident reports • Incident Report Forms • Notifications to insurance company • Exchanges with legal advisors. • Notifications to Health & Safety Authority (HSA)
Financial information, fees etc: Without this information, the school cannot process applications, make payments, or receive payment of monies (e.g. Book Rental or Course fees for e.g). After completion of the payments, the documentation is retained for audit and verification purposes.	• Information relating to payments from members (including fee support and fee waiver documentation).

Appendix 3 Categories of Recipients

Legal requirements where appropriate, the school may be obliged to seek advice and/or share personal data with *An Garda Síochána* where concerns arise. The school will also report matters of alleged criminal acts, criminal behaviour, criminal damage, etc., to allow prevention, detection and investigation of offences. Where there is a lawful basis for doing so, personal data may also be shared with the *Revenue Commissioners* and the *Workplace Relations Commission.*

Insurance data may be shared with the school's insurers where this is appropriate and proportionate. The school may also be obliged to share personal data with the *Health and Safety Authority*, for example, where this is required as part of an accident investigation. **Professional Advisors** some data may be shared with legal advisors (solicitors, etc.), financial advisors (accountants, etc.) and others such as school management advisors (JMB); this processing will only take place where it is considered appropriate, necessary and lawful.

Other Schools where the member transfers or applies for membership of another school the school may be asked to supply certain information about the member.

Other not-for-profit organisations limited data may be shared with recognised bodies who act to promote members' engagement with school-related activities, recognition of achievements, etc. This would include bodies promoting participation in commemorative events, etc. This data sharing will usually be based on consent.

Transfers Abroad In the event that personal data may be transferred outside the European Economic Area (EEA) the school will ensure that any such transfer, and any subsequent processing, is carried out in strict compliance with recognised safeguards or derogations (i.e., those approved by the Irish Data Protection Commission).

Implementing the Data Processing Principles

1. Accountability

(i) Accountability means that compliance with the data protection legislation is recognised as an important Board of Management responsibility as well as one shared by each school member and member of the wider school community.

(ii) Demonstrating Compliance Accountability imposes a requirement on the controller to demonstrate compliance with the other data processing principles (see Section 2 earlier: *Processing Principles*). This means that the Board of Management retains evidence to demonstrate the actions it has taken to comply with GDPR.

(iii)Record of Processing Activities As a data controller the school is required to prepare a record of any processing activities (ROPA) that it undertakes. This record should include the following information (GDPR Article 30):

- the purposes of the processing;
- a description of the categories of data subjects and personal data;
- the categories of recipients to whom the personal data will be disclosed;
- any transfers to a third country or international organisation, including suitable safeguards;

- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

(iv) Risk Assessment The school as data controller is required to consider any risks that may arise as a consequence of its processing activities. This assessment should consider both the likelihood and the severity of these risks and their potential impact on data subjects.[9]

(v) Data Protection Impact Assessment (DPIA) A DPIA is a type of risk assessment that is mandatory in specific circumstances (GDPR Article 35). The school will ensure that a DPIA is undertaken where this is appropriate, typically, where a new processing activity has the potential to have a high impact on individual privacy or rights. (The sharing of a member's political affiliation that is contrary to the school's constitution is an example of a processing activity that might trigger the need for a Data Protection Impact Assessment.) The purpose of undertaking a DPIA is to ensure that any risks associated with the new processing activity are identified and mitigated in an appropriate manner.

(vi) Security of Processing As a consequence of having assessed the risks associated with its processing activities, the school will implement appropriate *technical and organisational measures* to ensure a level of security appropriate to the risk. For example, these measures might include establishment of password procedures, protocols around device encryption, procedures governing access to special category data etc.

(vii) Data Protection by Design The school aims to apply the highest standards in terms of its approach to data protection. For example, Board of Management members will utilise a *Privacy by Design* approach when any activity that requires the processing of personal data is being planned or reviewed. This may mean implementing technical measures (e.g. security) and organisational measures (e.g. protocols).

(viii) Data Protection by Default A *Privacy by Default* approach means that minimal processing of personal data is the school's default position. In practice this means that only essential data will be collected from data subjects, and that within the school, access to this data will be carefully controlled and only provided to members where this is appropriate and necessary.

---

[9] GDPR Recital 75: The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(ix) Data Processing Agreements: the school will put written contracts in place with organisations that process data on its behalf (as required under GDPR Article 28). [10]

(x) Data Breach Records: the school will retain records that document its handling of any personal data breaches. These records will clearly set out the facts relating to any personal data breach, its effects and the remedial action taken. [11]

(xi) Member Awareness: All who are granted access to personal data that is under the control of the school have a duty to observe the data processing principles. The school will provide appropriate information and support so that Board of Management members may gain a clear understanding of these requirements.[12]

2. Lawful Processing

As part of its decision to collect, use or share personal data, the school as Controller will identify which of the lawful bases is applicable to each processing operation. In the absence of a lawful basis the personal data cannot be processed.

(i) Another set of data processing activities are undertaken in the public interest i.e. so that the school can operate safely and effectively. For example, information about the member may help the school to disassociate itself from certain media publications.

(ii) In some situations, for example the use of a disciplinary process, the school may rely on its legitimate interests to justify processing. In such cases the specific legitimate interests (e.g. health and safety, crime prevention, protection of school etc.) must be identified and notified to the data subjects[13].

(iii) There is also the possibility that processing can be justified in some circumstances to protect the Vital Interests of a data subject, or another person. For example, sharing some data subject data with emergency services might rely on this lawful basis.

(iv) Finally there is the option of using a data subject's consent as the lawful basis for processing personal data. The school will not rely on consent as the basis for processing personal data if another lawful condition is more appropriate. Consent will usually be

---

[10] A Data Processing Agreement may be provided as a set of agreed clauses or as an addendum to a broader *(Third Party) Service Agreement*.

[11] These record-keeping requirements are detailed under GDPR Article 33(5). Documentation need to be retained by the school setting out details of all data breaches that have occurred. This includes those that were adjudged not to require notification to the Data Protection Commission (in addition to data breaches that required formal DPC notification via https://forms.dataprotection.ie/report-a-breach-of-personal-data).

[12] All current and former employees of the school may be held accountable in relation to data processed by them during the performance of their duties. For example, employees acting in breach of the Data Protection Act 2018 could, in certain circumstances, be found to have committed a criminal offence.

[13] Data subjects have a right to object to processing that is undertaken based on legitimate interests. In such cases the Controller must demonstrate that there is an overriding need if the processing is to continue.

the lawful basis used by the school to legitimise the publication of members' photographs in print publications and electronic media.

3. Consent

Where consent is relied upon as the appropriate condition for lawful processing, then that consent must be freely given, specific, informed and unambiguous. All of these conditions must be satisfied for consent to be considered valid. There are a significant number of restrictions around using consent.

(i) A separate consent will be sought for each processing activity (together with appropriate guidance as necessary to ensure the data subject is informed).

(v) When asking for consent, the school will ensure that the request is not bundled together with other unrelated matters.

(vi) Consent requires some form of clear affirmative action (Silence or a pre-ticked box is not sufficient to constitute consent). Consent can be provided by means of an oral statement.

(vii) Consent must be as easy to withdraw as to give.

(viii) A record should be kept of how and when consent was given.

(ix) The school will take steps to ensure the consent is always freely given i.e. that it represents a genuine choice and that the data subject does not feel under an obligation to consent to processing.

(x) If the consent needs to be explicit, this means the school must minimise any future doubt about its validity. This will typically require the school to request and store a copy of a signed consent statement.

4. Special Category Data

Some personal data is defined as Special Category Data and the processing of such data is more strictly controlled. GDPR Article 9 identifies a limited number of conditions, one of which must be applicable if the processing of special category data is to be lawful.[14] Some of these processing conditions, those most relevant in the school context, are noted here.

(i) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the

[14] The Data Protection Act 2018 makes provision for some additional conditions that can legitimise the processing of special category data.

members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(ii) processing relates to personal data which are manifestly made public by the data subject;

(iii) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

(iv) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(v) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

5. Transparency

The school as Controller is obliged to act with *Transparency* when processing personal data. This requires the communication of specific information to individuals in advance of any processing of their personal data.[15]

(i) Transparency is usually achieved by providing the data subject with a written document known as a *Privacy Notice* or a *Privacy Statement*.[16] This notice will normally communicate:

- the name of the controller and their contact details;
- the categories of personal data being processed;
- the processing purposes and the underlying legal bases;
- any recipients (i.e. others with whom the data is shared/disclosed);
- any transfers to countries outside the EEA (and safeguards used);
- the storage period (or the criteria used to determine this);
- the rights of the data subject. [17]

[15] GDPR Articles 13 (or 14)

[16] Other terms in common use include *Fair Processing Notice* and *Data Protection Notice.*

[17] In the interests of transparency, the school should ensure that its preferred route for a rights request is identified clearly in *Privacy Notices* and elsewhere e.g. *"A data subject wishing to make an access request*

(ii) Transparency information should be provided in a manner that is concise and easy to understand. To best achieve this, the school may use a "layering" strategy to communicate information.[18] And, while a written *Privacy Notice* is the default mode, transparency information may also be communicated using other means, for example through the spoken word or through use of pictorial icons or video.

(iii) Privacy statements (include those used on school websites) should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data.

6. Purpose Limitation

(i) Personal data stored by the school has been provided by data subjects for a specified purpose or purposes.[19] Data must not be processed for any purpose that is incompatible with the original purpose or purposes.[20]

(ii) Retaining certain data (originally collected or created for a different purpose) with a view to adding to a school archive for public interest, scientific or historical research purposes or statistical purposes is acceptable subject to certain safeguards, most particularly the need to respect the privacy of the data subjects concerned.

7. Data Minimisation

As Controller, the school must ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In practice, this principle has a number of important implications illustrated in the examples below.

(i) The school should ensure, when data is being collected from data subjects, that this is limited to what is necessary for the completion of the duties. For example, where information is being collecting from members, this should be limited to whatever information is needed to operate the admissions process.

(ii) Data minimisation also requires that the sharing of members' data within the school should be carefully controlled. Board of Management members may require varying

---

should apply in writing to the GDPR Officer." Notwithstanding this, school members should be made aware that valid requests may be submitted in a variety of formats (i.e. not necessarily in writing).

[18] For example, where the first point of contact is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13 by way of further, different means, such as by sending a copy of the privacy policy by email and/or sending the data subject a link to the controller's layered online privacy statement/notice.

[19] This purpose is usually communicated to data subjects at the time of collection through providing them with a *Privacy Notice*.

[20] Data Protection Commission: *Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.*

levels of access to members' data. Access should be restricted to those who have a defined processing purpose. Board of Management members will not access personal data unless processing is essential to deliver on their role within the school.

(iii) school members will necessarily create personal data in the course of their association. However members should ensure that this processing is necessary and appropriate. For example, while it will often be necessary for Board of Management members to communicate information to each other by email, consideration should be given, on a case by case basis, as to whether it is necessary for personal data to be included in these communications.

(iv) Data sharing with external recipients should be continuously reviewed to ensure it is limited to that which is absolute necessary. This may mean, for example, that when the school is seeking professional advice, no personal data will be included in communications unless the disclosure of this information is essential.

8. Storage Limitation

Personal data is kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which it is being processed. Some personal data may be stored for longer periods insofar as the data is being processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(i) When deciding on appropriate retention periods, the school's practices will be informed by advice published by the relevant bodies (notably the Data Protection Commission, and the school management advisory bodies).

(ii) When documentation or computer files containing personal data are no longer required, the information is disposed of in a manner that respects the confidentiality of the data.

(iii) Data subjects are free to exercise a "right to erasure" at any time (also known as the "right to be forgotten", see *Data Subject Rights*).

(iv) Data should be stored in a secure manner that recognises controller obligations under GDPR and the Data Protection Act. This requires the school for example, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

9. Integrity and Confidentiality

Whenever personal data is processed by the school, technical and organisational measures are implemented to safeguard the privacy of data subjects. The school as controller is obliged to take its security responsibilities seriously, employing the most appropriate physical and technical measures, including members' training and awareness. These security procedures should be subject to regular review.

(i) Board of Management members are required to act at all times in a manner that helps to maintain the confidentiality of any data to which they have access. Guidance is important to help identify and reinforce appropriate protocols around data security.

(ii) The school is legally required to consider the risks to the data subject when any processing of personal data is taking place under its control. Any Risk Assessment should take particular account of the impact of incidents such as accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, the personal data.

(iii) As well considering the potential severity of any data incident, a risk assessment should also consider the likelihood of any incident occurring. In this way risks are evaluated on the basis of an objective assessment, by which it is established whether the data processing operations involve a risk or a high risk.[21]

(iv) The follow-on from any risk assessment is for the school to implement appropriate technical and organisational measures that ensure a level of security appropriate to the risk. *These measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected (GDPR Recital 83).*

(v) As well as processing activities undertaken by members, the school must also consider the risks associated with any processing that is being undertaken on behalf of the school by other individuals or organisations (Data Processors). Only processors who provide sufficient guarantees about the implementation of appropriate technical and organisational measures can be engaged.

Managing Rights Requests

10. Responding to rights requests

(i) The school will log the date of receipt and subsequent steps taken in response to any valid request. This may include asking the data subject to complete a dated written request in order to facilitate efficient processing of the request.

[21] The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk (GDPR Recital 76).

(xi) The school is obliged to confirm the identity of anyone making a rights request and, where there is any doubt on the issue of identification, will request official proof of identity (e.g. photographic identification such as a passport or driver's licence).[22]

(xii) If requests are manifestly unfounded or excessive[23], in particular because of their repetitive character, the school may refuse to act on the request.

(xiii) The school will need to confirm that sufficient information to locate the data requested has been supplied (particularly if footage/images are to be searched[24]). Where appropriate the school may contact the data subject if further details are needed.

(xiv) In responding to rights requests (e.g. data access requests) the school will ensure that all relevant manual[25] and automated systems (computers etc.) are checked.

(xv) The school will be conscious of the need to respond without undue delay and within the advised timeframes. A response will be made within one month of receipt of any request.[26]

(xvi) The school must be conscious of the restrictions that apply to rights requests.[27] Where unsure as to what information to disclose, the school reserves the right to seek legal advice.[28]

(xvii) Where a request is not being fulfilled, the data subject will be informed as to the reasons and the mechanism for lodging a complaint, including contact details for the Data Protection Commission.

---

[22] Where a subject access request is made via a third party (e.g. a solicitor) the school will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement.

[23] In such circumstances, the school must be able to demonstrate the manifestly unfounded or excessive character of a request.

[24] The school will always endeavour to respond to any access request within the stipulated time period. However a timely response can be greatly facilitated by provided (in writing to the AALEI) all necessary information such as date, time and location of any footage/images.

[25] Non-automated personal data that is held within a filing system or intended to form part of a filing system (GDPR Article 2).

[26] That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The school must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

[27] See for example GDPR Article 23 and Irish Data Protection Act 2018 S.56, S.60, S.61.

[28] Decisions around responding to data access requests will need to give due regard to rights and responsibilities that derive from other legislation.

(xviii) Where action has been taken by the school with regard to rectification, erasure or restriction of processing, the school will ensure that relevant recipients (i.e. those to whom the personal data has been disclosed) are appropriately informed.

11. Format of Information supplied in fulfilling a request

(i) The information will be provided in writing, or by other means, including where appropriate, by electronic means. (When requested by a data subject the information access may be provided in alternative means e.g. orally.)

(xix) The school will endeavour to ensure that information is provided in an intelligible and easily accessible format.

(xx) Where a request relates to video, then the school may offer to provide the materials in the form of a series of still images. If other people's images cannot be obscured, then it may not prove possible to provide access to the personal data.[29]

Reference sites

Data Protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

General Data Protection Regulation (GDPR official text) 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

General Data Protection Regulation (GDPR unofficial web version) 2016 https://gdpr-info.eu/

Irish Data Protection Commission https://www.dataprotection.ie/

Data Breach Report https://forms.dataprotection.ie/report-a-breach-of-personal-data

European Data Protection Board (EDPB) https://edpb.europa.eu/

EDPB Guidelines, Recommendations and Best Practices on GDPR https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Cyber Security Centre (Ireland) https://www.ncsc.gov.ie/

Cyber Security Centre (UK) https://www.ncsc.gov.uk/

---

[29] Where an image is of such poor quality that it does not relate to an identifiable individual, then it may not be considered to be personal data.

This policy and relevant procedures were adopted by the Board of Management on 2nd September 2024.

Signed:

Chairperson of Board of Management

Date: 2nd September 2024

Signed:

Principal/Secretary to the Board of Management

Date: 2nd September 2024

Date of next review: September 2025