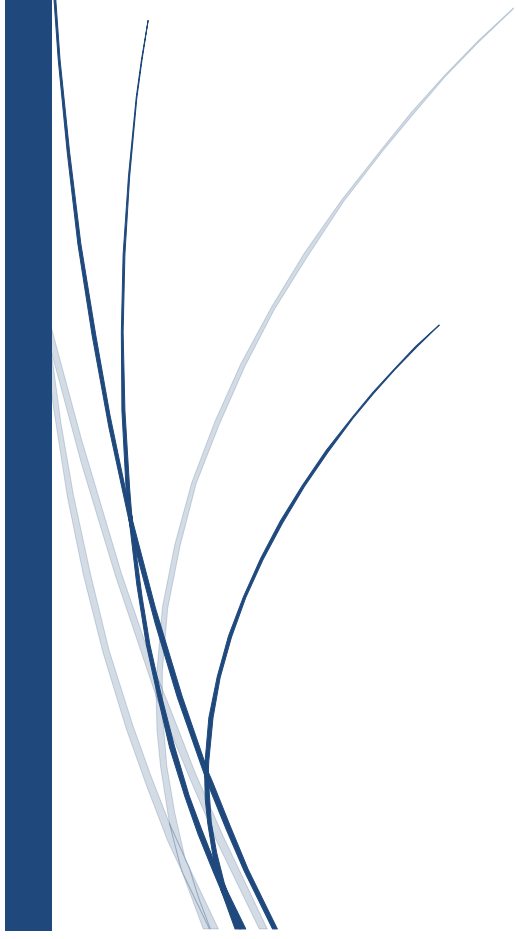
Data Protection Policy



SECRETARIAT OF SECONDARY SCHOOLS

Contents

1) Policy Statement Page 2

2) Purpose and Scope Page 2

3) Objectives Page 3

4) Processing Principles Page 3

5) Lawful Basis for Processing Personal Data Page 3

6) Processing Activities Undertaken by the Company Page 4

7) Recipients Page 5

8) Personal Data Breaches Page 6

9) Data Subject Rights Page 6

Appendix 1 Glossary Page 8

Appendix 2 Personal data and related Processing Purposes Page 9

Appendix 3 Categories of Recipients Page 11

Appendix 4 Implementing the Data Processing Principles Page 13

a) Accountability
b) Lawful Processing
c) Consent
d) Special Category Data
e) Transparency
f) Purpose Limitation
g) Data Minimisation
h) Storage Limitation
i) Integrity and Confidentiality

Appendix 5 Managing Data Subject Access Requests Page 19

Appendix 6 Reference Sites Page 20

1 Policy Statement

The Secretariat of Secondary Schools (hereafter "SSS" or "the Company") collects personal information to effectively carry out our business functions and activities and to provide services to voluntary secondary schools. Such data is collected from employees, volunteers, member schools, suppliers and consultants.

We may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however, we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), Irish data protection laws and any other relevant data protection laws and codes of practice.

2 Purpose and Scope

2.1 The purpose of this Data Protection Policy (hereafter the "Policy") is to support the Secretariat of Secondary Schools in 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.

2.2 This policy aids transparency by identifying how the Company 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.

2.3 The Irish *Data Protection Acts 1988 -2018* and the European *General Data Protection Regulation, 2016* are the primary legislative sources.[1] As such they impose statutory responsibilities on the Company as well as providing a number of fundamental rights for employees, service users, service providers and others in relation to personal data. The Company is obligated under the GDPR to protect, obtain, process, store and destroy personal data in compliance with its rules and principles.

2.4 The Company recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. The Policy applies to the Board of Directors, the Council of Association of Management of Catholic Secondary Schools (AMCSS), the Council of Joint Managerial Body (JMB), committee members, volunteers, all employees and applicants for staff positions within the Company, agency workers and consultants. Adherence to the Policy is mandatory.

2.5 Any amendments to the Policy will be communicated through the Company 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 the Policy or was otherwise communicated to you at the time that it was collected.

2.6 The Company is a data controller of personal data relating to its past, present and future staff, service users, and volunteers working with the Company. Formally, the statutory responsibility of Controller is assigned to the Board of Directors. The Assistant General Secretary (Corporate Services) has responsibility for co-ordinating the implementation of the Policy and for ensuring that all staff who handle or have access to personal data are familiar with their responsibilities.

Name	**Responsibility**
Board of Directors	Data Controller
Assistant General Secretary (CS)	Monitoring of the Implementation of the Policy
All staff and volunteers	Adherence to the data processing principles and awareness and respect for all personal data

[1] The Company 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 website etc.).

3 Objectives

We are committed to ensuring that personal data processed by the Company is done so in accordance with data protection legislation. The Company has developed the below objectives to meet our data protection obligations:

(i) Develop, implement, and maintain the Policy.
(ii) Provide training for the employees of the Company.
(iii) Protect the rights of individuals with regards to the processing of personal information.
(iv) Monitor and review current practice with a view to identifying gaps and non-compliance before they become a risk and we take mitigating actions where necessary.
(v) Keep up to date with developments in data protection legislation.
(vi) Have a robust Information Security System in place.
(vii) Be responsible for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection (as assigned to the Assistant General Secretary (Corporate Services)).

4 Processing Principles

4.1 **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 Company, including the storage of personal data, regardless of whether the records are processed by automated or manual means.

4.2 There are a number of fundamental principles that legally govern our treatment of personal data. The Company will ensure that all data processing is carried out in accordance with these principles, set out under GDPR, which 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**);
(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**).

4.3 GDPR also establishes **Accountability** as a core data processing principle. This places a statutory responsibility on the Company, as Data Controller, to be able to demonstrate compliance with the other principles i.e. the six data processing principles set out in the previous paragraph.

5 Lawful Basis for Processing Personal Data

5.1 Whenever the Company is processing personal data at least one of the following bases must apply if the processing is to be lawful:

(i) compliance with a legal obligation

[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).

(ii) necessity in the public interest
(iii) legitimate interests of the controller
(iv) contract
(v) consent
(vi) vital interests of the data subject

5.2 When processing **special category personal data**, the Company will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9.[3]

5.3 The lawful basis for processing personal data is explored further in Appendix 4.

6 Processing Activities Undertaken by the Company

6.1 **Record of Processing Activities** This section of the Policy sets out the purposes for which the Company collects and uses personal data for each of the various categories of personal data held (staff, service users, committee members, volunteers etc.).

6.2 **Staff Records** As well as records for existing members of staff (and former members of staff), records may also relate to applicants applying for positions within the Company. The purposes for which staff personal data is processed include the following:

(i) Recruitment and appointment
(ii) The management and administration of the business of the Company (now and in the future)
(iii) To comply with any obligations set out in contracts of employment
(iv) To facilitate the payment of staff and to calculate other benefits and entitlements (including illness benefit payment and leave)
(v) To facilitate pension payments (where relevant) in the future
(vi) Human resources management
(vii) Compliance with our obligations as an employer under relevant legislation including employment law, Health and Safety legislation etc.
(viii) To enable the Company to resolve disputes and defend litigation
(ix) To enable the Company to comply with reporting obligations to the Department of Education
(x) To enable the Company to comply with requirements set down by the Revenue Commissioners, the Garda Vetting Bureau, the Catholic Education Partnership, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
(xi) Compliance with Company law and other legislation relevant to the Company.

6.3 **Service users data (i.e. schools).** The purposes for which school data is processed include the following:

(i) To communicate relevant information to schools
(ii) To deliver an efficient advisory service to schools
(iii) To provide training for school personnel
(iv) To respond to queries raised by individual schools
(v) To collect annual subscriptions and fees for training sessions
(vi) To comply with legislative or administrative requirements
(vii) To operate the regional AMCSS structure
(viii) To enable the Company to comply with requirements set down by the Department of Education
(ix) To facilitate the recruitment of volunteers and committee members
(x) To comply with regulations relating to school accounts
(xi) To facilitate the conduct of research

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

6.4 **Committee Members and Volunteers** The purposes for which personal data is processed include the following:

(i) To communicate relevant information including invites to meetings etc
(ii) To ensure the effective running of the Councils of JMB/AMCSS
(iii) To facilitate the work of sub-committees
(iv) To pay expenses
(v) To operate the regional AMCSS structure
(vi) To enable the Company to comply with requirements set down by the Charities Regulatory Authority

6.5 **Board of Directors Records** are retained in accordance with the CRA Governance Code and other applicable legislation. Minutes of Board of Directors meetings record attendance, items discussed, and decisions taken. Board of Directors business is considered confidential to the members of the Board. Names and contact details of directors are retained.

6.6 **Financial Records** This information is required for routine management and administration of the Company's financial affairs, including the collection of subscription fees, the payment of invoices, the payment of salaries, expenses, and pensions, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

7 Recipients

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

7.2 **Data Sharing Guidelines**

(i) From time to time the Company may disclose personal data to third parties or allow third parties to access specific personal data under its control. By way of example, An Garda Síochána could 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 Company 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 transfers to other bodies arises as a consequence of a legal obligation, and the majority of the data recipients are data controllers in their own right (e.g. the Department of Education). As such their actions will be governed by national and European data protection legislation as well their own organisational policies.[4]

(iv) Some of the Company's operations require support from specialist service providers. For example, the Company 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.

8 Personal Data Breaches

8.1 **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.

[4] The Data Protection Policy of the Department of Education can be viewed on its website (www.education.ie).

8.2 **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 theft or fraud, financial loss, damage to reputation, loss of confidentiality etc.

(ii) In addition to any detrimental impact on individual data subjects, a data breach can also cause serious damage to the Company. This can include reputational damage as well as exposing the Company 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 Company and/or for participating individuals.[5]

8.3 **Responding to a Data Breach**

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

(ii) As soon as the Company 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 Company believes that there is a risk to the affected individuals, the Company 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 Company will inform those individuals without undue delay.

9 Data Subject Rights

9.1 **Your Rights** Personal Data will be processed by the Company in a manner that is respectful of the rights of data subjects. Under GDPR these include[6]

(i) the right to information
(ii) the right of access
(iii) the right to rectification
(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.

9.2 **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 Company (info@jmb.ie)

9.3 **Right of Access** You are entitled to see any information we hold about you. The Company 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 Company in responding to a right of access must ensure that it does not adversely affect the rights of others.

9.4 **Right to rectification** If you believe that the Company 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.

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

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

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

9.6 **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.

9.7 **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.

9.8 **Right to object** Data subjects have the right to object when processing is based on the Company's legitimate interests or relates to a task carried out in the public interest (e.g. the processing of data in the interest of the Voluntary Secondary Sector e.g. Research Commission).

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

9.10 **Right to withdraw consent** In cases where the Company 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.

9.11 **Limitations on Rights** While the Company will always facilitate the exercise of your rights, it is recognised that they are not unconditional: the Company may need to give consideration to other obligations.[7]

9.12 **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 Assistant General Secretary (Corporate Services) who is responsible for operational oversight of this policy.

(ii) A matter that is still unresolved may then be referred to the Chairperson, Secretariat of Secondary Schools, Emmet House, Dundrum Road, Milltown, Dublin 14.

(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
E-mail	info@dataprotection.ie
Post	Data Protection Commission
	Canal House, Station Road
	Portarlington, Co. Laois
	R32 AP23

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

Appendix 1. GLOSSARY

Child - a person under the age of 18 years. Children are deemed as vulnerable under GDPR and merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

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 Company.

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 (<u>but does not include</u> an employee of a controller who processes such data in the course of his or her employment).

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 category 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. The management and administration of the business of the Company (now and in the future);	
Staff **Purposes may include:** (i) Recruitment and appointment (ii) Compliance with our obligations as an employer: ○ to facilitate the payment of staff, and to calculate other benefits/ entitlements (including the calculation of pension payments, entitlements and/or redundancy payments where relevant); ○ to facilitate pension payments in the future; ○ to facilitate the monitoring of annual leave in compliance with the Organisation of Working Time Act, 1997 ○ human resources management; ○ recording duties and responsibilities and changes to same; ○ to enable the Company to provide a safe working environment (including complying with its responsibilities under the *Safety, Health and Welfare at Work Act. 2005*); ○ to contact a next of kin in the case of an emergency. (iii) To enable the Company to resolve disputes and defend legislation. (iv) To enable the Company to comply with reporting obligations to the Department of Education (v) to enable the Company to comply with requirements set down by the CRA, the CRO, the Revenue Commissioners, the Garda Vetting Bureau, the Catholic Education Partnership, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies; (vi) and for compliance with Company law and other legislation relevant to the Company;	The personal data we collect includes but is not limited to your: name; date of birth; address; contact details; telephone number; gender; CV and qualifications; Teaching Council Registration or registration with any other professional or accrediting body; PPS number; financial data, images, medical health and occupational health data, immigration/work-visa information; information relating to recruitment; promotions and appointment processes; salary and pensions details; emergency contact details; general job description; letter of appointment; records of CPD attended; records of health and safety training; accident reports, notifications to the HSA, communication with legal advisors, notifications to the insurers, leave of absence applications (job share, career break, maternity leave); annual leave records; records documenting employee's authorisation for non-statutory payroll deduction; expenses recorded and reimbursed, disciplinary records; performance management records, records of HR related meetings; copies of allegations and complaints; industrial relations correspondence including minutes of meetings; Dignity at Work files including allegations of bullying; Grievance case files; OHS referral letters, medical reports, assessment and absence records; Employee Assistance Programme referral letters; and files relating to the Workplace Relations Commission hearings and Court processes.
2. To carry out the role of a recognised school management body and to provide management, compliance, and advisory services	
School information Purposes may include: (i) Advisory Service ○ Issuing of bulletins to principals, deputy principals and chairpersons ○ Provision of a response to written communication received from schools.	The school data we collect includes but is not limited to: ○ The name, postal address, telephone number, email address, and website details of the school ○ The name of the trustees of the school ○ The names, addresses, telephone numbers and email addresses of the school principal, deputy principal/(s), chairperson of the board of

○ Provision of financial advice (FSSU) ○ Provision of procurement advice (SPU) ○ Provision of advice relating to school building (ii) Vetting (iii) Training (iv) Educational research (v) Recruitment of committee members and volunteers (vi) Operation of committees and the Councils of AMCSS and JMB (vii) Operation of the regional structure (viii) Website and promotional materials (ix) Security (x) Financial management	management, school secretary and accounts secretary/bursar. ○ The names, postal and email addresses, telephone numbers, car registration details of members of committees and members of the Councils of JMB/AMCSS. ○ Information required to fulfil the vetting requirements as set out in Circular Letter 31/2016 and 16/2017 including: name, date of birth, address, email address, contact number, role for which the individual is being vetted and disclosures ○ The names, postal and email addresses, telephone numbers, car registration details of attendees at JMB training and events. ○ Information required to respond to queries submitted by the principal/deputy principal or chairperson of an individual school. ○ Photos and digital images of attendees at training events and conferences ○ Images which appear on the camera at the front door of Emmet House. ○ Record of complaints ○ Records of levies and payments received and refunds processed. ○ Documentation for audit and verification purposes.

Appendix 3. CATEGORIES OF RECIPIENTS

Department of Education (DE) The Company is required to provide some data to the Department of Education. This transfer of data is primarily made to facilitate the payment of grants.

National Vetting Bureau The Company is required to provide data to the National Vetting Bureau to comply with the requirements of Circular Letter 31/2016, and Circular Letter 16/2017

Legal Obligations The Company is required to provide personal data to certain recipients in order to comply with its legal obligations, where appropriate, particularly in relation to compliance with its tax obligations. The Company may share personal data with An Garda Síochána where concerns arise in relation to child protection. The Company will report matters of a criminal nature to An Garda Síochána also. Where there is a lawful basis for doing so, personal data may also be shared with the *Revenue Commissioners* and/or the *Workplace Relations Commission (WRC).* The Company may also be obliged to share personal data with the Health and Safety Authority.

Insurance Data may be shared with the Company's insurers where this is appropriate and proportionate.

Professional Advisors Personal data may be shared with legal advisors (e.g. solicitors), financial advisors (e.g. pension administrators, accountants) and other professional advisors (e.g. consultants) where it is considered appropriate, necessary and lawful.

Service Providers In some circumstances the Company has appointed third parties to undertake processing activities on its behalf. These Data Processors have provided guarantees that their processing satisfies the requirements of the General Data Protection Regulation. The Company has implemented written contractual agreements with these entities to ensure that the rights of data subjects receive an appropriate level of protection. Third party service providers include (but are not limited to) the following:

IT Systems and Services

ERS Computing	Business Pals House, Unit 5, Block 8, Blanchardstown, Dublin
Software Design & Development	9 Brentwood Cresent, Earls Court, Dunmore East Road, Waterford X91 HD2K
SystemNet Communications Ltd	Unit 123 Tallaght Business Centre, Whitestown Industrial Estate, Dublin D24 RFC2
Privacy Engine	77 Sir John Rogerson's Quay, Dublin 2, D02 F540
Zenark Ltd	77 Lower Camden Street, Dublin, D02 XE80
Fusio	26 Strand Street, Great North City, Dublin
Microsoft 365	Managed by ERS
MS Teams	Managed by ERS
One Drive	Managed by ERS
Zoom	Managed by IMS 1st Floor Ashbourne Hall dock Road Limerick
Inventise	Prince of Wales Terrace, 1 Quinsborough Road, Bray, Co. Wicklow A98 CK20
GetOnline Pro Ltd	No. 17 Nutgrove Community Enterprise Centre, Nutgrove Way, Rathfarnham, Dublin 14

Information Management Systems

Team Project	Unit AG, M4 Business Park, Celbridge, Co. Kildare
Super Office	CRM Unit 17 Cranfield Innovation Centre, University Way, Cranfield, United Kingdom

Legal Services

Mason Hayes & Curran,	South Bank House, Barrow Street, Dublin 4, D04 TR29
Lewis Silkin Ireland,	Fitzwillam Court, Office Suite 505 – 506, Lesson Close, Dublin, D02 YW24

Payroll & Pensions

Advance Systems	4L The Square Industrial Complex Unit, Tallaght, Dublin 24
Sage	Sage Ireland, 1 Central Park, Leopardstown, Dublin 18, D18 NH10
AIB	Clonskeagh, 60 Bothar Chluain Sceach, Farranboley, Dublin 14
Irish Life	Irish Life Centre, Abbey Street, North City, Dublin 1

Recruitment

Gilligan Black Recruitment	40 Lower Lesson Street, Dublin 2

Transfers Abroad In the event that personal data may be transferred outside the European Economic Area (EEA) the Company 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).

Appendix 4. IMPLEMENTING THE DATA PROCESSING PRINCIPLES

1. Accountability

(i) Accountability means that compliance with the data protection legislation is recognised as an important responsibility of the Company as well as one shared by each employee and volunteer within the organisation.

(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 Company retains evidence to demonstrate the actions it has taken to comply with GDPR.

(iii) Company Policies An important way for the Company to demonstrate accountability is through the agreement and implementation of appropriate policies. In addition to publishing a *Data Protection Policy* this may include developing other policies to address some or all of the following areas (i) Data Breaches (iii) Data Access Requests (iv) Record Storage and Retention (v) Data Processing Agreements.

(iv) Record of Processing Activities As an organisation with less than 250 employees, the Company does not maintain records of our processing activities. However, we continue to review all such activities to ensure that we will begin to record such information as detailed in GDPR Article 30 where:

- We employ 250 or more employees
- Processing personal data could result in a risk to the rights and freedoms of individuals
- The processing is not occasional
- We process special categories of data or criminal convictions and offences

(v) Risk Assessment The Company, 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.[8]

(vi) Data Protection Impact Assessment (DPIA) A DPIA is a type of risk assessment that is mandatory in specific circumstances (GDPR Article 35). The Company 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 installation of an electronic system for the management of vetting 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.

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

(viii) Data Protection by Design The Company aims to apply the highest standards in terms of its approach to data protection. For example, staff 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

[8] 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.

implementing technical measures (e.g. security) and organisational measures (e.g. protocols and training).

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

(x) Data Processing Agreements: The Company will put written contracts in place with organisations that process data on its behalf (as required under GDPR Article 28). [9]

(xi) Data Breach Records: The Company 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. [10]

(xii) Staff Awareness and Training All who are granted access to personal data that is under the control of the Company have a duty to observe the data processing principles. The Company will provide appropriate information, training and support so that staff may gain a clear understanding of these requirements.[11]

2. Lawful Processing

As part of its decision to collect, use or share personal data, the Company 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) Some of Company's data processing activities rely on legal obligations. These tasks are undertaken because the Company must comply with Irish (or European) law[12]. For example, there is a legislative basis underpinning the sharing of specific employee data with the Revenue Commissioners.

(ii) Another set of data processing activities are undertaken in the public interest, so that the Company can effectively fulfil its advisory function or representation role as a recognised management body.

(iii) In some situations, for example the use of CCTV, the Company 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 Company property etc.) must be identified and notified to the data subjects[13].

(iv) Contract will provide a lawful basis for most processing of data by the Company. For example, the processing of employee data and data received from schools may rely on this lawful basis.

(v) 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 (e.g. sharing personal data with emergency services).

(vi) Finally there is the option of using a data subject's consent as the lawful basis for processing personal data. The Company will not rely on consent as the basis for processing personal data if another lawful condition is more appropriate. Consent will usually be the lawful basis used by the Company to legitimise the publication of individual and group photographs in print publications and electronic media.

---

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

[10] These record-keeping requirements are detailed under GDPR Article 33(5). Documentation setting out details of all data breaches that have occurred will be retained by the Company. 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).

[11] All current and former employees of the Company 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.

[12] For example, the *Education Act 1998* and the Companies Act 2014.

[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.

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).

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

(iii) 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.

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

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

(vi) The Company 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.

(vii) If the consent needs to be explicit, this means the Company must minimise any future doubt about its validity. This will typically require the Company 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. In a SSS context this will occur whenever data that relates to an employee'shealth is being processed. 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 Company context, are noted here.

(i) Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law. This condition could provide an appropriate basis for processing of data relating to employee health e.g. proportionate sharing of special category data to ensure the Company is compliant with provisions in health, safety and welfare legislation.

(ii) Processing is necessary for the assessment of the working capacity of an employee; or for the provision of health or social care or treatment on the basis of Union or Member State law.

(iii) Processing is based on explicit consent. Where the Company is processing biometric data for identification purposes (e.g. facial image recognition or the use of fingerprint systems). In these instances, a data subject will be able to withhold consent without suffering any detriment, the Company will provide access to an alternative processing option which is not reliant on biometric data.

5. Transparency

The Company 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);

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

[15] GDPR Articles 13 (or 14)

[16] Other terms in common use include *Fair Processing Notice* and *Data Protection Notice*. Schools may prepare a number of different Privacy Notices for use in different contexts. For example, a *Website Privacy Notice*, may relate specifically to personal data that is collected via the school website.

- 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]

(ii) Transparency information should be provided in a manner that is concise and easy to understand. To best achieve this, the Company 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 the Company 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 Company 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 the Company 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 Company 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 Company 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 collected from schools it means that it is usually not appropriate for the Company to seek the home address of the principal/deputy principal or other staff members.

(ii) Data minimisation also requires that the sharing of personal data within the Company should be carefully controlled. Members of staff may require varying levels of access to personal data and reports. Access should be restricted to those who have a defined processing purpose. Staff will not access personal data unless processing is essential to deliver on their role within the Company.

(iii) Staff will necessarily create personal data in the course of their duties. However, employees should ensure that this processing is necessary and appropriate. For example, while it will often be necessary for staff 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 Company is seeking

[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 should apply in writing to the Principal."* Notwithstanding this, school staff 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.*

professional advice or providing 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 Company's practices will be informed by advice published by the relevant bodies (notably the Department of Education and the Data Protection Commission).

(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 Company 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 Company, technical and organisational measures are implemented to safeguard the privacy of data subjects. The Company as controller is obliged to take its security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness. These security procedures should be subject to regular review.

(i) Employees 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 and training are important to help identify and reinforce appropriate protocols around data security.

(ii) The Company 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 Company 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 staff, the Company must also consider the risks associated with any processing that is being undertaken on behalf of the Company 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.

[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).

(vi) The important contribution that organisational policies can make to better compliance with the Accountability principle was previously highlighted. Similarly, the implementation of agreed policies and protocols around data security is very helpful. Some possible areas are listed below.

- Company ICT policy
- Acceptable User Polices for employees, board members, volunteers etc.
- Accessing Company data from home
- Password policy
- Use of staff personal devices at work
- Use of Company devices outside work
- Social Media Policy
- Cloud Based Systems

Appendix 5. MANAGING DATA SUBJECT ACCESS REQUESTS (DSARs)

1. Responding to rights requests

(i) The Company 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 an *Access Request Form* in order to facilitate efficient processing of the request. There is no charge for this process.[22]

(ii) The Company 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).[23]

(iii) If requests are manifestly unfounded or excessive[24], in particular because of their repetitive character, the Company may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

(iv) The Company will need to confirm that sufficient information to locate the data requested has been supplied. Where appropriate the Company may contact the data subject if further details are needed.

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

(vi) The Company 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]

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

(viii) 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.

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

2. 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.)

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

(iii) Where a request relates to video, then the Company 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]

---

[22] The Company may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information. Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

[23] Where a subject access request is made via a third party (e.g. a solicitor) the Company 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.

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

[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 Company 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, not least Article 42A of the Irish Constitution which recognises and affirms the natural and imprescriptible rights of all children. Examples of other factors that might need to be considered include: any court orders relating to parental access or responsibility that may apply; any duty of confidence owed to the child or young person; any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment); any detriment to the child or young person if individuals with parental responsibility cannot access this information; and any views the child or young person has on whether their parents should have access to information about them.

[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.

Appendix 6. 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

DES Data Protection Page https://www.education.ie/en/The-Department/Data-Protection/Information.html

PDST Technology in Education https://www.pdsttechnologyineducation.ie

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

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