

Ashton School

DATA PROTECTION

POLICY

DATA PROTECTION POLICY

1	Purpose and Scope	1
2	Processing Principles	2
3	Lawful Basis for Processing Personal Data.....	3
4	Processing Activities Undertaken by the School.....	3
5	Recipients.....	4
6	Personal Data Breaches.....	5
7	Data Subject Rights	6
	Appendix 1. Glossary.....	8

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 students, parents/guardians and staff and others) in relation to personal data.

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 school website etc.).

- 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 staff, boards of management, patrons, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions 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.
- 1.6 The school is a *data controller of personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. Formally, the statutory responsibility of Controller is assigned to the 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.

Name	Responsibility
Board of Management	Data Controller
Principal	Implementation of Policy
All Staff	Adherence to the Data Processing Principles
Entire School Community	Awareness and Respect for all Personal Data

2 Processing Principles

- 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 processed²; (**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 Lawful Basis for Processing Personal Data

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 Processing Activities Undertaken by the School

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 (student, staff, parent, etc).

4.2 **Student Records** The purposes for processing student personal data include the following:⁴

- (i) to provide information prior to application/enrolment;
- (ii) to determine whether an applicant satisfies the school's admission criteria;
- (iii) to comprehend the educational, social, physical and emotional needs of the student;
- (iv) to deliver an education appropriate to the needs of the student;
- (v) to ensure that any student seeking an exemption from Irish meets the criteria;
- (vi) to ensure that students benefit from relevant additional educational or financial supports;
- (vii) to contact parents/guardians in case of emergency or in the case of school closure;
- (viii) to monitor progress and to provide a sound basis for advising students and parents/guardians;
- (ix) to inform parents/guardians of their child's educational progress etc.;
- (x) to communicate information about, and record participation in, school events etc.;
- (xi) to compile yearbooks, establish a school website, and to keep a record of the history of the school;
- (xii) to comply with legislative or administrative requirements;

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

⁴ The type of personal data being processed by the school and the purposes for which this data is being processed is likely to be subject to revision from time to time. For example, changes in curriculum or legislation may require adjustments in the personal data processing.

- (xiii) to furnish documentation/ information about the student to the Department of Education and Skills, the State Exams Commission, the National Council for Special Education, TUSLA, and others in compliance with law and directions issued by government departments.
- 4.3 **Parent/Guardian Records** The school does not keep personal files for parents or guardians. However, information about, or correspondence with, parents may be held in the files for each student. This information shall be treated in the same way as any other information in the student file.
- 4.4 **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 school, trainee teachers and teachers under probation. The purposes for which staff personal data is processed include the following:
- (i) the management and administration of school business (now and in the future);
 - (ii) to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant);
 - (iii) to facilitate pension payments in the future;
 - (iv) human resources management;
 - (v) recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.;
 - (vi) to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the *Safety, Health and Welfare at Work Act. 2005*);
 - (vii) to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies;
 - (viii) and for compliance with legislation relevant to the school.
- 4.5 **Board of Management Records** Board of Management records are kept in accordance with the Education Act 1998 and other applicable legislation. 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.
- 4.6 **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.
- 4.7 **CCTV Records** The school processes personal data in the form of recorded CCTV images. We use CCTV for the following purposes:
- (i) to secure and protect the school's premises and assets;
 - (ii) to deter crime and anti-social behaviour;
 - (iii) to assist in the investigation, detection, and prosecution of offences;
 - (iv) to monitor areas in which cash and/or goods are handled;
 - (v) to deter bullying and/or harassment;
 - (vi) to maintain good order and ensure the school's Code of Behaviour is respected;
 - (vii) to provide a safe environment for all staff and students;
 - (viii) for the taking and defence of litigation;
 - (ix) for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and where the recordings may be capable of resolving that dispute.

5 Recipients

- 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.

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 Gardai 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.

3 Personal Data Breaches

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 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.

⁵ The Data Protection Policy of the Department of Education and Skills can be viewed on its website (www.education.ie).

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

4 Data Subject Rights

- 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 include⁷
- (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.
- 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.
- 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.

If you are a student who is subject to estimated marks, and you make a data access request to the school for your estimated marks before the issue of results, the school will advise the following:

- that in line with section 56 of the Data Protection Act, it is not possible to respond to the request at present, and
 - that the request will be taken to have been made on the later of either the date of the first publication of the results of the ‘examination’ (i.e. the Accredited Grades process), or the date of the request.
- 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 CCTV data may rely on the school’s legitimate interest in maintaining a safe and secure school building). The school must demonstrate compelling legitimate grounds if such processing is to continue.

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

- 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 Principal 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 Chairperson c/o school.
 - (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 Portarlinton, Co. Laois R32 AP23
Website	www.dataprotection.ie

⁸ 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 School.

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 (but does not include 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 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.