Introduction
Mary Immaculate High School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and GDPR legislation. Changes to data protection legislation will therefore be monitored and implemented to ensure Mary Immaculate High School remains fully compliant with all requirements set out by the Information Commissioner's Office. This means as a school we will ensure data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- accurate and where necessary kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data has been obtained
- processed in a manner which ensures appropriate security of personal data

This policy is supplemental to any other school policies in respect of information management. Mary Immaculate High School collects and uses certain types of personal information to provide pupils with an education and other associated functions. This includes information on current, past, and prospective; pupils, parents, staff, contractors, partners, and others who come into contact with us as a school. This information must be dealt with properly no matter how it is collected, recorded, and used – whether on paper, by computer or recorded through any other means. This means the requirements of this policy are mandatory for all staff employed by the school and for any third party contracted to provide further services the school may require.

Roles and Responsibilities
Mary Immaculate High School strongly recognises the importance of ensuring the security and safekeeping of personal data. The school is committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them. Therefore, everyone within the school community has a direct role and responsibility to play in ensuring data protections and guidelines are fully adhered to. The roles and responsibilities of the school community are outlined below:

Board of Governors
The headteacher and at least another member of the board of governors should be aware of the procedures to be followed in the event of a serious data breach taking place. It is also the direct responsibility of the board of governors to ensure that there is a system in place to allow for the monitoring and support of those in the school community who carry out the GDPR role.

Headteacher
The Headteacher has a direct responsibility for data protection and as such will report to the Board of Governors on GDPR matters. The Headteacher will act as the contact point for any requests from individuals to access their personal data. The Headteacher is the registered IPO Data Protection Officer. However, the day-to-day responsibility for GDPR is delegated to the school's GDPR Officer. The Headteacher is therefore responsible for ensuring the GDPR Officer is given sufficient support and training to carry out their role effectively.

GDPR Officer
The GDPR Officer takes the day-to-day responsibilities for data protection away from the Headteacher and has a direct role in establishing, implementing, and reviewing the school's GDPR policies. The GDPR Officer is expected to:

- Take the lead in monitoring and identifying any GDPR incidents which occur and liaise with the Senior Leadership Team and any relevant bodies in the school community to deal with these incidents quickly and effectively

- Ensure that all staff are aware of the procedures that need to be followed in the event of a data breach
- Provide training and advice for staff for key GDPR matters
- Meet regularly with the Network Manager and Business Manager to discuss current GDPR matters
- Produce, review, and monitor the school's GDPR literature
- Producing and maintaining the school's privacy notice (Appendix A)
- Carrying out DIPAs related to teaching and learning matters
- Maintaining the Information Asset Register in relation to teaching and learning matters

Business Manager
It is important to remember compliance within data protection procedures within the school community goes far beyond the remit of teaching staff and as such the Business Manager is responsible for ensuring:

- Personal information is held no longer than is necessary and as such appropriate records management procedures of policies are in place to comply with this principle
- All data held in any form of media (paper, tape, electronic) is only passed to a disposal partner with demonstrable competence in providing secure disposal services.
- Any data destroyed or eradicated to agreed levels meets recognised national standards, with confirmation at completion of the disposal process
- Ensuring the ongoing confidentiality, integrity and resilience of processing systems and services

Network Manager
The Network Manager is expected to support the GDPR officer in their role and help them investigate any data breaches which may occur. The Network Manager is therefore expected to:

- Ensure all access to personal information on school systems is strictly controlled through the use of password and username hierarchical structures
- All devices within the school community are encrypted wherever possible
- Ensure the technical infrastructure of the school's IT systems are secure and not open to misuse or malicious attack
- Make sure that access to the network and to school devices only takes place through a properly enforced password protection system
- They keep up to date with technical information related to GDPR to support the GDPR Officer to effectively carry out their role and to inform and update other users as required
- Review audit logs on a regular basis to ensure all user behaviour within school computer systems appears within normal limits
- They implement and maintain the School Technical Security Policy
- Review regularly the school ICT and security systems
- Ensure all software, apps and websites used within the school community are fully compliant with GDPR guidelines
- Disposal of IT assets holding data follows ICO guidelines
- Carryout regular testing, assessing and evaluating of the effectiveness of technical software for ensuring the security of processing data
- Restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Maintaining the Information Asset Register in relation to non-teaching and learning matters

All Staff
All staff are responsible for ensuring:

- Paper-based records and portable electronic devices such as laptops and iPads that contain personal information are kept in a secure location when not in use
- Papers containing confidential personal information isn't left on office and classroom desks, on staffroom tables or pinned to notice boards where there is general access

- Passwords are at least eight characters long and contain both letters and numbers and are not written down
- Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely
- Personal data, including sensitive pupil data, is not removed from school premises without clear authorisation from the Headteacher
- Personal devices are not used to store or process any pupil data
- Data is not shared with anyone other than people that has defined the need to know
- All personal information and data is treated with care and security
- They seek further guidance from the GDPR Officer if they are unsure or have any queries in relation to how comply fully with GDPR guidelines
- If you are emailing someone internally and especially externally outside of the school community and the email contains sensitive data, the email is encrypted, and any files attached are password protected
- Any unwanted paperwork is disposed of via the school's confidential waste procedures
- Compliance with this policy, breach of compliance may result in disciplinary action being taken
- If a school device or paperwork is lost, it is reported immediately to the GDPR Officer and Head Teacher

Teaching Staff
The delivery of education requires data to be gathered to assess, monitor, and inform pupil progress. It is therefore vital teaching staff ensure:

- When classrooms are left unattended, the teacher computer / laptop is locked
- Mark-books, pupil work, exam papers or exercise books are always kept secure, whether in school or at home or in transit
- That when meeting pupils or parents they are not able to view your screen unless the content is directly related to them
- When using any system with data displayed, they make sure that the projector does not display the information for pupils to see
- The only devices used for teaching and learning purposes are the devices purchased and issued by Mary Immaculate High School
- When transporting a laptop, tablet device or paperwork to and from school it is securely stored in the boot of the vehicle and not visible from the outside

Personal Data
Personal data about pupils is not to be disclosed to third parties without the consent of a child's parent or carer, unless it is obliged by law or in the best interest of the child. However, data may be disclosed to the following third parties without consent:

- **Other schools -** If a pupil transfers from Mary Immaculate High School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. Any transfer of data will take place through the use of cardiff.gov email domain. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary.
- **Examination authorities –** Data may be provided to examination authorities for registration purposes, to allow pupils at our school to sit examinations set by external exam bodies.
- **Health authorities -** As obliged under health legislation, the school may pass on information regarding the health of children to monitor and avoid the spread of contagious diseases in the interest of public health.
- **Police and courts -** If a situation arises where a criminal investigation is being carried out, information maybe forwarded on to the police to aid their investigation and as such we will pass information onto courts as and when it is required.
- **Children services -** To protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Right to Rectification and Erasure
GDPR gives individuals the right to have their personal data rectified if it is inaccurate or incomplete. The school will make it easy for individuals to access and correct their personal information. Where a request for rectification is received, the statutory time limit for response and implementation is one month. This can be extended by two months where the request for rectification is complex.

The right to erasure is also known as "the right to be forgotten" and enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. There are some specific circumstances where the right to erasure does not apply, for example where safeguarding and social services legislation prevents this. Therefore, any requests for the erasure of data will be dealt with on a situation-by-situation approach and the decision of the Head Teacher and Governing Body in such matters will be final.

Subject Access Requests
All individuals whose data is held by us as an organisation, have a legal right to request access to their data or information about what data is being held. As an organisation we shall respond to such requests within one working month of receipt. Requests should be made in writing for the attention of the Headteacher and proof of identification should be provided by the requestor. This request will then be reviewed and referred if necessary to the Business Manager or GDPR Officer for further advice or guidance.

Individual Rights
Mary Immaculate High School recognises individuals' rights as fundamental and therefore endorses the enhancement of individual data rights as set out in legislation. All requests for personal information will be dealt with in accordance with the individual's statutory rights. Queries regarding the School's processing of personal data will be dealt with promptly and courteously.

The GDPR framework provides the following rights for individuals:

1. The right to be informed (Privacy notices).
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision-making and profiling

The right to obtain personal information (subject access) is exempted in respect of Education Data if its release would be likely to cause harm to the physical or mental health of the data subject or another individual. The right of access also does not apply to child abuse data to the extent that the application of the provision would not be in the best interests of the data subject.

Digital Imaging Technology
Digital imaging technology can add real value to both teaching and learning within the school environment and as such images and videos of staff and pupils may be captured at appropriate times and as part of educational activities for use in school or for wider publication. However, unless prior consent from parents / carers, pupils or staff has been given, the school shall not utilise such images for publication or communication purposes to external sources. Pupils aged 13 and above have the right to access their own information (within legal bounds) and can remove right to use images and videos.

Legal Basis for Processing Data
Personal information will only be processed where there is a lawful basis for doing so. Under the GDPR framework there are six available lawful bases for processing data, a summary of each is listed below:

- **Consent -** the individual has given clear consent for you to process their personal data for a specific purpose

- **Contract -** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- **Legal obligation -** the processing is necessary for you to comply with the law.
- **Vital interests -** the processing is necessary to protect someone's life
- **Public task -** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in the law
- **Legitimate interests -** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

The basis which is used within the processing of data is fully dependent on the situation and more than one basis may apply to a situation. In the event of uncertainty as to whether a basis applies further guidance should be sought from the GDPR Officer before the process of obtaining or processing any data takes place.

Privacy Notices
The school will, at point of collection, unless an appropriate exemption applies, inform individuals of the specific purpose or purposes for which the school will use their personal information. To ensure the information required by Article 13 of the GDPR framework is adhered to Appendix A contains a copy of the school's privacy notice which is also available on the school website. The privacy notice has been written in a clear way in which pupils can understand. Where a pupil is below 13 years of age consent must be given by the holder of parental responsibility for the child.

Data Sharing
At Mary Immaculate High School, we work with many third-party organisations such as contractors, agents, partners, consultants, etc. When working with these organisations to share and process data we will ensure there is be a written agreement between the school and the third party confirming that they have appropriate technical and organisational security measures in place to safeguard the personal data and as such third parties will act on the instructions of the school. The school will ensure that only contractors who can provide "sufficient guarantees" that the requirements of the GDPR framework will be met and the rights of individuals are protected will be authorised to work with ourselves as an organisation.

DPIA New Technology
Technology constantly evolves and as such with that evolvement it presents new risks to us an organisation. Therefore, when introducing new systems, software, applications, and devices to the school community a DIPA must be carried out before they are used. A Data Protection Impact Assessment is a tool which can help identify the most effective way in which we can ensure the new tool complies fully with data protection obligations and meet individuals' expectations of privacy. DPIAs also allow us as a school to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur if a data breach was to take place.

The carrying out of DIPAs is the responsibility of both the Business Manager and GDPR Officer who may consult with further stakeholders to assess the risks new systems, software, apps and devices may bring to the school community. Any decisions made by either the Business Manager or GDPR Officer in such matters is final.

The only systems, software, apps and devices which may be used in the school community must be the ones listed on the School's Information Asset Register spreadsheet. The GDPR Officer, Network Manager and Business Manager all responsible for co-ordinating and maintaining. If staff wish for new items to added to the authorised list this register contains, they must at first liaise with the Network Manager to explore the viability and advantages it may bring to the school community.

Data Breaches
The GDPR framework introduces a duty on us a school community to report certain types of data breaches to the Information Commissioner's Office.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data, for example, unauthorised access to school systems is also a breach.

Breaches of personal or sensitive data shall be notified immediately to the Head Teacher who will then contact the Data Protection Officer for Cardiff City Council who will then assess if the ICO needs to be contacted for further advice and guidance.

If the breach is likely to result in a high risk to the rights and freedoms of persons involved, we will inform the data subject without undue delay.

Complaints
Complaints in relation to processing of personal data or any queries regarding this policy should be addressed in the first instance to the school's GDPR officer and then if necessary, should be brought to the attention of the Headteacher.

Policy Review Date: December 2021
Next Review December 2022

Appendices

Appendix A – School Privacy Notice

Appendix A
Privacy Notice

Introduction
We collect and use pupil information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6(1)(c) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

We use pupil data in the following ways:

- As part of our admissions process
- To support pupil teaching and learning
- To monitor and report on pupil progress to provide appropriate pastoral care
- To assess the quality of our services
- To comply with the law regarding data sharing
- To access our school meals, payments and school communication system
- To support you to decide what to do after you leave school

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and contact details)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as lessons attended, number of absences and absence reasons)
- National curriculum assessment results, external examination and/or assessment results, special educational needs information, relevant medical information, behavior logs.
- Biometric fingerprints for school meals

Collecting pupil information
Whilst most of the information you provide to us is mandatory, some of it is provided to us on a voluntary basis. To comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us, or if you have a choice in this.

Storing pupil information
Mary Immaculate High School keeps information about you on school computer systems, devices and sometimes on paper.

We hold your education records securely (computerised and paper) in accordance with guidance issued by the Local Authority regarding document retention i.e. to comply with legal requirements e.g. date of birth plus 25 years for prime documents linked to safeguarding, SEN, Educational Psychology, School Admissions, EWS and 7 years for PLASC counts, class counts, SEN registers, School Action Plans, GEMS intervention referrals, admissions reports, school meals reports etc. after which they are safely destroyed.

We may also share your personal data with other internal and external partners and agencies for the purposes of progressing you onto further education, employment, or training. The partners / agencies that we will share with are Cardiff Council, Careers Wales, St David's Sixth Form College and local Training Providers".

Access to the school's IT and Data Systems is restricted to authorised individuals only and is underpinned and protected by our ICT and E-Safety Policy and Acceptable Usage Policies. Access is logged and routinely monitored to protect users and the integrity and security of systems and data.

Mary Immaculate High School adheres to the following retention periods for computer held personal data:

- Pupil user areas and mailboxes are retained for a period of 1 calendar year
- Staff user areas and mailboxes are retained for a period of 5 calendar years
- System backups are retained for a period of 1 calendar year and web filter logs for a period of 30 days except for print logs which are held for a period of 1 calendar year and 1 month
- CCTV is operated on site using internal and external cameras and footage is retained for a period of 30 days
- Recordings of live lessons / videos is used for training purposes and sharing of best practice and retained for a period of 5 calendar years.
- Teams meetings may be recorded and kept for 24 hours
- Phone records / messages are retained for a period of 3 months
- Biometric fingerprint information is destroyed as pupils leave school
- Basic pupil information is retained on our SIMS system (School Management Information System) and retained for a period of 25 years

Where data resides on third party systems e.g. Microsoft Office 365 contracts exist to ensure data security, integrity and retention periods match legislation with our own in-house systems.

All system backups are encrypted and are held in multiple, physical secure locations as part of the school's disaster recovery policy.

There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it is the only way we can make sure you stay safe and healthy, are legally required to do so or the data is required for operational purposes.

Paper records are held in lockable cabinets. All visitors to site have a photograph taken and are logged into an electronic visitors access system. Control to areas where records are stored is restricted – pupils and visitors are not permitted to access any such area unless required and under the supervision of a staff member.

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Welsh Assembly Government on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. To find out more about the data collection requirements placed on us by the Welsh Assembly Government please visit - http://gov.wales/topics/educationandskills/schoolshome/schooldata

The school will, on an annual basis, share individual Data Collection Sheets with you to ensure that our records are accurate and up to date.

Requests for Information

All recorded information held by the school may be subject to requests under the Freedom of Information Act 2000, and the General Data Protection Regulations. If you would like to submit a Freedom of Information / Subject Access Request the request should be made in writing for the attention of the Headteacher and proof of identification should be provided by the requestor.

Your Rights

The Data Protection Act / GDPR gives you a number of rights. Please note not all of your rights are absolute and we will need to consider your request upon receipt. You do however have the right to request:

- to have your data rectified if it is inaccurate or incomplete
- to have your data erased
- to restrict the processing of your data
- to exercise your right to data portability
- to object to the processing for the purposes of direct marketing, profiling and automated decision making

If you have a concern about the way in which we are collecting or using your personal data, you should raise your concern with us in the first instance by contacting the school's GDPR Officer.

Contact

If you would like to discuss anything in this privacy notice, please contact Adam Speight who is the school GDPR Officer – aspeight@maryimmaculate.cardiff.sch.uk