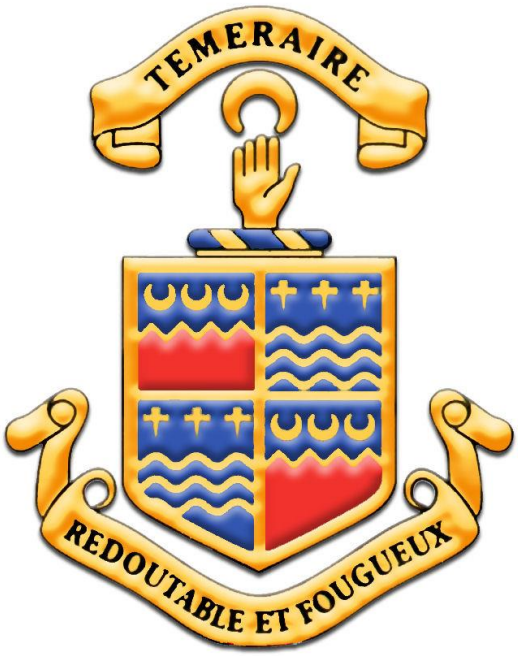
THE HARVEY GRAMMAR SCHOOL



Data Protection Policy

May 2018

Introduction

The Harvey Grammar School Academy is committed to a policy of protecting the rights and privacy of all individuals, including students, staff and others, for whom it holds personal data in order to fulfill its role as an Academy.

Personal data is any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

This personal data includes information about current, past and prospective employees; pupils and their parents/carers; governors; and business contacts such as suppliers. All such data, whether held in manual or electronic filing systems or both, will be collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully in accordance with the requirements of the **General Data Protection Regulation (GDPR)**. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

We collect and use pupil information under Section 537A of the Education Act 1996, Section 175 of the Education Act 2002 and Section 83 of the Children Act 1989.

We collect and use staff information under Sections 113 and 114 of the Education Act 2005 and Section 4(2) of the Rehabilitation of Offenders Act 1974.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Department for Education (DfE). The data subject will be made aware how and with whom their data is shared through the Privacy Notice.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the core principles of GDPR.

Data Controller

The Harvey Grammar School is the Data Controller, which means that it determines what purpose personal information held, will be used for. It is also responsible for notifying the Information Commissioner (ICO) of the data it holds or is likely to hold, and the general purpose that this data will be used for. The school's registration number is Z546437X.

Principles

In accordance with the requirements outlined in the GDPR, personal data:

1. shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
2. shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. shall be accurate and, where necessary, kept up to date;
5. shall not be kept for longer than is necessary for that purpose;
6. shall be processed and shared in accordance with the data subject's rights;
7. shall be 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;
8. shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Compliance and Accountability

As the Controller, the school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy notices and policies.

The school will implement measures that meet the principles of data protection by design and default, such as:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

Records of activities relating to higher risk processing will be maintained.

Data protection impact assessments will be used, where appropriate.

The school will set out clear procedures for responding to subject access requests.

The school will treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

All staff and governors will receive adequate training on data protection and the GDPR.

The school ensures that all processors used to handle personal data have a written contract outlining responsibilities. Contracts will include requiring the processor to take appropriate measures to ensure the security of processing.

This policy applies to all staff and students of The Harvey Grammar School. A breach of the rules and procedures identified in this policy or the GDPR itself may lead to disciplinary action being taken.

As a matter of best practice, other agencies and individuals working with the school and who have access to personal information will be expected to read and comply with this policy.

Data Protection Officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the Governors and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the schools compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

Where an existing employee is appointed to the role of DPO the school will ensure that their duties are compatible with the duties of the DPO and do not lead to a conflict of interest.

The individual appointed as DPO will have professional experience and knowledge of data protection law.

The DPO will report to the highest level of management

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

Lawful Processing

The legal bases for processing data are as follows:

- **Consent:** The member of staff/student/parent has given clear consent for the school of process their personal data for specific purpose. This can be withdrawn by the individual at any time.
- **Contract:** the processing is necessary for the member of staff's/prospective applicant's employment contract
- **Legal obligation:** the processing is necessary for the school to comply with the law (not including contractual obligations)
- **Legitimate Interests:** the processing is necessary for the legitimate interests of a third party (emergency contacts) unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests.

Use of Biometric Information

In addition to GDPR, The Protection of Freedoms Act 2012, includes measures that will affect schools that use biometric recognition systems, such as fingerprint identification. The school ensures consent of a parent is given prior to taking and processing the child's biometric data. It is treated with appropriate care in line with GDPR, and alternative means for accessing services are provided where consent has not been given or is withdrawn.

Rights of data subjects

All individuals for whom the school holds personal data (**data subjects**) are entitled to:

- **The right to be informed**: A Privacy Notice is issued to all data subjects within one month of obtaining data.
- **The right of access**: Individuals have the right to submit a subject access request to obtain their personal information.
- **The right of rectification**: individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
- **The right to erasure**: Individuals can request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- **The right to restrict processing**: Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction e.g. verifying the accuracy of the data.
- **The right to data portability**: re-use automated personal data for the individuals own purposes across different services e.g. Common Transfer Files between schools.
- **The right to object**: Individuals can object to direct marketing, processing for purposes of scientific or historical purposes and statistics or processing based on legitimate interests.

All of these rights should be actioned within one month of the request.

Data Breaches

A personal data breach refers to a breach of security, which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Where a breach is likely to result in a risk to the rights and freedoms of individuals the ICO will be notified within 72 hours of becoming aware of it. Where the breach is likely to result in a 'high risk' to the rights and freedoms of individuals, those concerned will also be notified.

Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels, meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Policy Updates

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to data protection legislation.