UK General Data Protection Regulations (GDPR) and Data Protection Policy

Policy Reference Number:	Issue Date: October 2021	Review Date: October 2022

Contents

1. Purpose

The Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) are the legislation that protect personal privacy and uphold individual rights. This policy will ensure that personal information is dealt with correctly, in accordance with the legislation. It will provide information about Marchant-Holliday School's approach to collecting and processing personal data in the course of its day-to-day work. It will also provide information as to the rights of those individuals who data we hold. The policy applies to personal data regardless of the way it is used, recorded or stored and whether it is held in paper files or electronically.

Terminology: Data is a raw and unorganised fact that is required to be processed to make it meaningful whereas information is a set of data that is processed in a meaningful way according to the given requirement.

2. Policy Objectives

The school as Data Controller will comply with its obligations under the legislation. The school is committed to being clear and transparent about how it obtains and uses personal information and will ensure that data subjects are aware of their rights under the legislation.

All staff have a general understanding of the legislation which will inform their decisions about how and what personal data is collected, used, stored and ultimately, deleted.

The senior management team will understand the retention schedule for different types of data and information and will ensure they are stored securely in an organised manner.

The school will appoint a Data Protection Officer to ensure that all staff adhere to the policy and to update the policy.

3. Scope of the Policy

The school holds a variety of personal data with personal data being defined as information that can be used to identify a living individual. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. Personal information also includes an identifier such as a name, identification number or location data.

The school continually collects personal data on pupils, staff, Governors, parents and carers and data from unsuccessful job candidates.

Special Categories of personal data refers to sensitive personal data about an individual such as race, nationality, ethnic origin, politics, religion, health or sexual orientation

4. Data Protection Principles

There are specific principles set out in the legislation that must be adhered to when processing personal data.

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner ***(lawfulness, fairness and transparency)***
- Collected for specified, explicit and legitimated purposes and not further processed in a manner that is incompatible with those purposes **(*purpose limitation)***
- Adequate, relevant and limited to what is necessary on relation to the purposes for which they are processed **(*data minimisation)***
- Accurate and where necessary, kept up to date **(*accuracy)***
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the data is processed ***(storage limitation)***
- Processed in a manner that ensures appropriate security of the data ***(integrity and confidentiality)***

Transfer limitation means that personal data shall not be transferred outside the UK unless that country ensures an adequate level of protection for the rights and freedoms of the data subjects.

5. Lawful Basis for Processing Personal Data

Under UK GDPR legislation, there are six lawful reasons that a school can use to justify why it needs to process data. The decision as to which lawful basis applies must be documented to demonstrate compliance with data protection principles.

Public task

This basis is that the school is processing data to carry out a task in the public interest e.g. to deliver education or to fulfil official functions that have a clear basis in law

Legal obligation

This basis is that the school is processing data to comply with the law e.g. health and safety requirements

Fulfilling a contract

This basis is that the school is processing data to comply with their obligations under a contract.

Vital interests

This basis is that the school needs to process data to save someone's life.

Legitimate interests

When determining whether legitimate interests is the most appropriate basis for lawful processing, a legitimate interest assessment should be carried out. Where a significant privacy impact is identified, a Data Protection Impact Assessment should also be carried out – see Appendix

Consent:

The school has received clear consent to process data for one or more specific purposes e.g. fundraising, marketing etc.

Consent may need to be refreshed if personal data is to be processed data for a different purpose which was not disclosed when the data subject first consented.

Processing Sensitive Personal Data

Sensitive personal data is data which reveals an individual's identity such as race, ethnic origin, religion sexuality etc. The processing of sensitive personal information, known also as 'special categories of personal data' is prohibited unless a lawful condition for processing is identified. Sensitive personal information will only be processed if there is a lawful basis for doing so.
We process special categories of personal data and criminal offence data to meet our obligations under employment law.

Unless the school can rely on another legal basis for processing, explicit consent is usually required for processing sensitive data. Evidence of consent would need to be captured to ensure compliance.

Data held about individuals will not be kept for longer than necessary – see Appendix: ***Retention Schedule***

6. Privacy Notice

We use Privacy Notices to inform data subjects whose personal data we collect about how we use their information and the lawful basis on which we are processing it. There is a privacy notice on the vacancies section of the school website for employment candidates. There is also a privacy notice in the Parents and Carers section of the website detailing how we capture their personal data.

7. Rights of Individuals

Individuals have the right to ask what personal data the school is holding on them and to gain access to the personal data by making a Subject Access Request (SAR). An SAR must be made in writing to the school by letter or email. Identity verification will be required before any access is made.

In most cases, SAR's will be responded to within one calendar month of receipt. Requests made outside of term time may take longer to respond to.

A fee is not charged for the providing a copies of information except where the school has assessed the request as being manifestly unfounded or excessive or where further copies of the same information are requested.

If the school refuses to respond to an SAR, it will explain why and advise of the right to complain to the Information Commissioner's Office (ICO).

Additional Individual Rights

In addition to the rights of access described above, individuals also have other rights:

- **Right to rectification**: the right to have inaccurate personal data rectified, or completed, if incomplete
- **Right to erasure:** the right to have personal data erased (also known as the 'right to be forgotten')
- **Right to restrict processing:** the right to request the restriction or suppression of personal data i.e. limiting the ways in which the school can use data
- **Right to data portability** allows individuals to obtain and reuse their personal data for their own purposes across different services
- **Right to object:** the right to object to processing based on legitimate interests or the performance of a task in the public interest. This also covers direct marketing as well as processing for purposes of scientific or historical research and statistics
- **Rights relating to automated decision-making including profiling:** automated individual decision making refers to making a decision solely by automated means without any human involvement. Profiling refers to automated processing of personal data to evaluate certain things about an individual.

The school does not currently use automated decision making in any of its processing activities

8. Authorised Disclosures

The school will only disclose data about individuals with their consent. However, there are circumstances where the school may need to disclose data without explicit consent.

These circumstances are limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and fulfil its statutory obligations
- Pupil data disclosed to authorised recipients in respect of a pupil's health, safety and welfare
- Pupil data disclosed to families in respect of their child's progress, achievements, attendance, attitude or general demeanour
- Staff data disclosed to relevant authorities, e.g. HMRC and pension providers
- Unavoidable disclosures e.g. Prodigy, the outsourced IT support company remotely accessing PCs

9. Data and Computer Security

The school undertakes to ensure personal data security by several methods.

Physical security:

Building security measures such as alarms, locks and electronic key pads are in place. Visitors to school are required to sign in and out, to wear identification badges whilst on site, and accompanied where appropriate.

Computer security – general

The school's web filters are secure and up to date. New security releases are updated on all networked ICT hardware.

Computer Security - Users

All computer users have individual log on and passwords which are only known to themselves. The log on and passwords are created by Prodigy IT Solutions, the school's outsourced IT support company. Prodigy do not keep a record of the passwords that are created.

All computerised data is organised into folders on the server with different levels of, dependent upon user authority. All portable devices such as Chromebooks, Laptops, Tablets and IPads are also security password protected.

The main server is located in a room adjacent to the Head Teacher's office and so has restricted access. The back-up server is located in a room adjacent to the ICT Suite with restricted key access. Computerised backs up are carried out daily to the Cloud.

Email Security

All email accounts have multi-factor authorisation enabled so access is secure. SMT and the PA to the Senior Management team send encrypted confidential data by email.

Procedural Security:

The school has the following safeguards in place:

- We have a designated Data Protection Officer (DPO)
- All staff are issued with Data Protection Guidelines and are aware of their obligations
- A deliberate breach of the Data Protection Guidelines will be treated as a disciplinary matter
- All confidential waste documents are placed in security sacks for collection and shredding by a third-party private company

10. Documentation and Records

The school has a GDPR mapping document which records details of all data subject information held, the type of data held, the physical location of the data and the applicable lawful basis as to why the data is being held. The school also has a retention schedule documenting how long certain types of data should be kept.

The mapping document details the following information and linked information:

- School Function e.g. Finance, Human Resources etc.
- Data Subject e.g. staff, governor, pupil, contractor etc.
- Personal Data Categories e.g. first name, last name, address, date of birth etc.
- Method of Collection e.g. job application form, new starter form, pupil admission form etc.
- Purpose of Data Collection e.g. recruitment, lesson observations, record-keeping etc.
- Data Processor e.g. Headteacher, SENCo, Finance & ICT Manager etc.
- Third Party Data Sharing E.g. Local Authority, HMRC, Pension Providers
- Staff Access
- Data Protection Impact Assessments (DPIA)
- Records of Consent

11. GDPR Awareness and Training

All staff and Governors are issued with a GDPR Guidance document to make them aware of GDPR issues and how the school keeps compliant. The guidance will be updated in response to changes in legislation and re-issued.

The school will arrange GDPR training from an external provider to ensure that staff and Governors are aware of how GDPR legislation applies to school activities.

12. Data Breaches

The DPO will log any and investigate any data breaches. The DPO, in conjunction with SMT will decide if it is necessary to report at breach to the Information Commissioner's Office (ICO). A breach needs to be reported within 72 hours of the DPO being made aware that the breach has occurred.

If a breach it likely to result in a high risk to the rights and freedoms of individuals, the school will inform those concerned directly.

13. Contact Us

A questions or concerns about Data Protection are directed to Data Protection Officer.

14. Complaints

The school takes any complaints about the collection and use of personal data seriously. If a data subject thinks that the collection or use of personal information is unfair, misleading or inappropriate, or has any other concern about our data processing, this is raised with the school in the first instance. If the data subject isn't satisfied with the school response, they are entitled to a complaint to the ICO.

Appendix

UK General Data Protection Regulations (GDPR) Guidance for Staff and Governors

UK GDPR and Data Protection Guidelines for Staff and Governors

Contents

1. Purpose

The Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) are the legislation that protect personal privacy and uphold individual rights.

This school needs to ensure that personal data is dealt with correctly, in accordance with the legislation. This guidance provides information about Marchant-Holliday School's approach to collecting and processing personal data in the course of its day-to-day work. It will also provide information as to the rights of those individuals who data we hold. The guidance applies to personal data regardless of the way it is used, recorded or stored and whether it is held in paper files or electronically.

Data is classed as raw unorganised fact whereas information is the data processed in a meaningful way according to the given requirement e.g. reports.

2. Scope of the guidance

The school holds a variety of personal data with personal data being defined as information that can be used to identify a living individual. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. Personal information also includes an identifier such as a name, identification number or location data.

Special Categories of personal data refers to sensitive personal data about an individual such as race, nationality, ethnic origin, politics, religion, health or sexual orientation

The guidance should be read in conjunction with the Data Security and ICT Usage document as we need to ensure that data we capture and store during the course of the school day, e.g. photographs and videos of pupils on iPads and cameras is not in contravention of the data protection legislation.

3. Data collection

We gather and hold data on staff, pupils, parents and carers, governors and unsuccessful job applicants. We have a retention schedule which documents how long we can keep certain types of data e.g. for unsuccessful job applicants, we only hold application forms for 6 months after a post had closed.

We collect personal data from staff via their employment application forms. We collection personal data about pupils, parents and carers from school admission documents and legal documents such as the Education, Health and Care Plan (EHCP).

We have to be very mindful of the privacy, legality and security of the data that we hold in school.

4. Data protection principles

There are specific principles set out in the data protection legislation that we must adhere to when processing personal data.

The personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimated purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary on 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 individuals for no longer than is necessary for the purposes for which the data is processed
- Processed in a manner that ensures appropriate security of the data

Transfer limitation isn't applicable for the data we hold at school but means that personal data shall not be transferred outside the UK unless that country ensures an adequate level of protection for the rights and freedoms of the data subjects. This is more applicable now that the UK is no longer part of the EU.

5. Lawful basis for processing personal data

Under UK GDPR legislation, there are six lawful reasons that a school can use to justify why it needs to process data. The decision as to which lawful basis applies is documented to demonstrate compliance with data protection principles.

Public task
This basis is that the school is processing data to carry out a task in the public interest e.g. to deliver education or to fulfil official functions that have a clear basis in law

Legal obligation
This basis is that the school is processing data to comply with the law e.g. health and safety requirements

Fulfilling a contract
This basis is that the school is processing data to comply with their obligations under a contract.

Vital interests
This basis is that the school needs to process data to save someone's life.

Legitimate interests

When determining whether legitimate interests is the most appropriate basis for lawful processing, a legitimate interest assessment should be carried out. Where a significant privacy impact is identified, a Data Protection Impact Assessment should also be carried out – see Appendix

Consent:
The school has received clear consent to process data for one or more specific purposes e.g. fundraising, marketing etc.

Consent may need to be refreshed if personal data is to be processed data for a different purpose which was not disclosed when the data subject first consented.

Processing Sensitive Personal Data

Sensitive personal data is data which reveals an individual's identity such as race, ethnic origin, religion sexuality etc. The processing of sensitive personal information, known also as 'special categories of personal data' is prohibited unless a lawful condition for processing is identified.

Sensitive personal information will only be processed if there is a lawful basis for doing so. The school processes special categories of personal data and criminal offence data to meet our obligations under employment law.

Unless the school can rely on another legal basis for processing, explicit consent is usually required for processing sensitive data. Evidence of consent would need to be captured to ensure compliance.

6. Privacy notice

We use Privacy Notices to inform data subjects whose personal data we collect about how we use their information and the lawful basis on which we are processing it. There is a privacy notice on the vacancies section of the school website for employment candidates. This notice explains what happens with the data we capture during the recruitment process and what happens to it.

There is also a Privacy Notice in the Parents and Carers section of the new website detailing how we capture their personal data and their son's data and again, what happens to it.

7. Rights of individuals

All individuals have the right to ask what personal data the school is holding on them and to gain access to the personal data by making a Subject Access Request (SAR). An SAR must be made in writing to the school by letter or email. Identity verification will be required before any access is made.

In most cases, SAR's will be responded to within one calendar month of receipt. Requests made outside of term time may take longer to respond to.

A fee is not charged for the providing a copies of information except where the school has assessed the request as being manifestly unfounded or excessive or where further copies of the same information are requested.

If the school refuses to respond to an SAR, it will explain why and advise of the right to complain to the Information Commissioner's Office (ICO).

Additional individual rights

In addition to the rights of access described above, individuals also have other rights:

- **Right to rectification**: the right to have inaccurate personal data rectified, or completed, if incomplete
- **Right to erasure:** the right to have personal data erased (also known as the 'right to be forgotten')
- **Right to restrict processing:** the right to request the restriction or suppression of personal data i.e. limiting the ways in which the school can use data
- **Right to data portability** allows individuals to obtain and reuse their personal data for their own purposes across different services
- **Right to object:** the right to object to processing based on legitimate interests or the performance of a task in the public interest. This also covers direct marketing as well as processing for purposes of scientific or historical research and statistics
- **Rights relating to automated decision-making including profiling:** automated individual decision making refers to making a decision solely by automated means without any human involvement. Profiling refers to automated processing of personal data to evaluate certain things about an individual.

The school does not currently use automated decision making in any of its processing activities

8. Authorised disclosures

The school will only disclose data about individuals with their consent. However, there are circumstances where the school may need to disclose data without explicit consent e.g. in the course of payroll processing, data is disclosed to HMRC and pension providers.

9. Data and computer security

The school has the following measures to ensure personal data security:

Physical security
Building security measures such as alarms, locks and electronic key pads are in place. Visitors to school are required to sign in and out, to wear identification badges whilst on site, and accompanied where appropriate.

Computer security – general
The school's web filters are secure and up to date. New security releases are updated on all networked ICT hardware.

Computer Security - Users
All computer users have individual log on and passwords which are only known to themselves. The log on and passwords are created by Prodigy IT Solutions, the school's outsourced IT support company. Prodigy do not keep a record of the passwords that are created.

All computerised data is organised into folders on the server with different levels of, dependent upon user authority. All portable devices such as Chromebooks, Laptops, Tablets and IPads are also security password protected.

The main server is located in a room adjacent to the Head Teacher's office and so has restricted access. The back-up server is located in a room adjacent to the ICT Suite with restricted key access. Computerised backs up are carried out daily to the Cloud.

Email Security
All email accounts have multi-factor authorisation enabled so access is secure. SMT and the PA to the Senior Management team send encrypted confidential data by email .

Procedural Security:
The school has the following safeguards in place:

- We have a designated Data Protection Officer (DPO) – Gary Paul, Finance & ICT Manager
- All staff are issued with Data Protection Guidelines and are aware of their obligations
- A deliberate breach of the Data Protection Guidelines will be treated as a disciplinary matter
- All confidential waste documents are placed in security sacks for collection and shredding by a third-party private company

10. Documentation and records

The school has a GDPR mapping document which records details of all data subject information held, the type of data held, the physical location of the data and the applicable lawful basis as to why the data is being held. The school also has a retention schedule documenting how long certain types of data should be kept.

The mapping document details the following information and linked information:

- School Function e.g. Finance, Human Resources etc.
- Data Subject e.g. staff, governor, pupil, contractor etc.
- Personal Data Categories e.g. first name, last name, address, date of birth etc.
- Method of Collection e.g. job application form, new starter form, pupil admission form etc.
- Purpose of Data Collection e.g. recruitment, lesson observations, record-keeping etc.
- Data Processor e.g. Headteacher, SENCo, Finance Manager etc.
- Third Party Data Sharing E.g. Local Authority, HMRC, Pension Providers
- Staff Access
- Data Protection Impact Assessments (DPIA)
- Records of Consent

11. Data breaches

The DPO will log any and investigate any data breaches. The DPO, in conjunction with SMT will decide if it is necessary to report at breach to the Information Commissioner's Office (ICO). A breach needs to be reported within 72 hours of the DPO being made aware that the breach has occurred. For example, if payroll was processed for a particular month and members of staff received the wrong payslips, this would be a significant breach. The DPO would also needs to inform all members of staff directly affected.

12. Areas of concern

Use of pupil images

We need to ensure that we abide by the information provided on parental consent forms and not take, use or store images and/or videos of pupils for whom we don't have permission to do so. We also needs to ensure that all staff are aware of who the pupils are for whom we don't have consent

We also need to ensure that we don't store and display images of pupils who no longer attend school as this is contravention of the lawful bases for processing data.

Emails

Pupils are referred to by their initial in internal and external email correspondence.

Photocopying and printing

Although, we have security regarding printouts and photocopies to the main printer in Reception, we need to ensure that confidential information about staff and pupils is not sent to other printers which remains uncollected and visible to a wider audience than the original intention.

Electronic storage

IPads, laptops, cameras and tablets are classed as portable electronic devices. We need to ensure that pupil images are regularly removed from these devices and appropriately stored e.g. on portable hard drives.

We must also ensure that access rights to certain type of confidential data on the server are maintained and that confidential information is stored unencrypted on the P: drive, e.g. staff payslips, appraisal information, sickness forms etc.

13. Complaints

The school takes any complaints about the collection and use of personal data seriously. If a member of staff thinks that the collection or use of personal information is unfair, misleading or inappropriate, or has any other concern about our data processing, this is raised with the school in the first instance.

If the member of staff isn't satisfied with the school response, they are entitled to a complaint to the ICO.