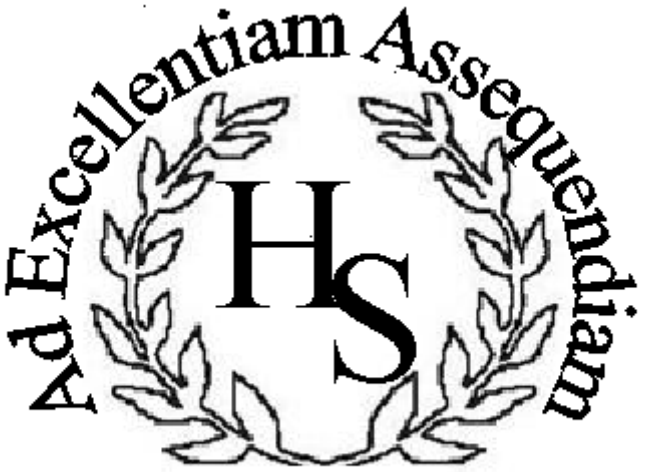

HEATON SCHOOL

Data Protection Policy

TO BE REVIEWED SEPTEMBER 2021

Heaton School Policy Record

School Accessibility Policy Agreed at:

FGB 14.2.2019

Signed and Approved by:

Headteacher ---------- (Signature)

---------- (Name)

---------- (Date)

Chair of Committee---------- (Signature)

---------- (Name)

---------- (Date)

To Be Reviewed: September 2021

Designated person: J Curtis, Headteacher

Produced by	Becky Swan – Deputy Data Protection Officer, SMBC
Date approved and agreed	November 2018
Review Date	May 2019
Date Amended	

Contents

1. Introduction

Heaton School takes its responsibilities with regard to the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) seriously. This policy sets out how the school manages those responsibilities.

Heaton School is committed to data protection by design and regards the lawful and appropriate processing of personal and special category data as an integral part of its purpose.

This policy sets out the accountability and responsibilities of the School, its staff and its students to comply fully with the provisions of GDPR DPA.

Heaton School holds and processes personal data about individuals such as employees, students and others, defined as 'data subjects'. Such data must only be processed in accordance with GDPR and the DPA.

This policy therefore seeks to ensure that we:

1. Are clear about how personal data must be processed and the Schools expectations for all those who process personal data on its behalf;

2. Comply with the data protection law and with good practice;

3. Protect the Schools reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights;

4. Protect the School from risks of personal data breaches and other breaches of data protection law.

This policy applies to all personal data the school processes regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the Schools behalf must read it. A failure to comply with this policy may result in disciplinary action.

The School has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with GDPR and the DPA.

The Digital Economy Act 2017 requires every data controller (i.e. organisation) in the UK to pay a fee to the Information Commissioner's Office (ICO). The schools registration number is Z6287446

2. GDPR sets out key principles for processing data

When processing personal data, all staff should be guided by the principles laid out below. The school must be able to demonstrate compliance with these principles;

Personal data must be:

1. Processed **lawfully**, **fairly** and in a **transparent** manner in relation to individuals.

2. **Purpose limitation** - 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

3. **Data minimisation** - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. **Accuracy** - 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

5. **Storage limitation -** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals

6. **Integrity and confidentiality (security) -** 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

The controller shall be accountable for, and be able to demonstrate compliance with the above principles.

3. The lawful basis for processing

The first principle, as referred to above, requires that you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies.

If no lawful basis applies to your processing, your processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.

The individual's right to be informed under Article 13 and 14 requires Heaton School to provide people with information about your lawful basis for processing. This means you need to include these details in your privacy notice.

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

2. **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.

3. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

4. **Vital interests**: the processing is necessary to protect someone's life.

5. **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 law.

6. **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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

4. Accountability

The School must implement and evidence appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

1. Appointing a suitably qualified DPO;

2. Implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects (further information may be found below);

3. Integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;

4. Training staff on compliance with Data Protection and keeping a record accordingly; and

5. Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

5. Responsibilities

1. School responsibilities

The School, as data controller is responsible for establishing policies and procedures in order to comply with data protection.

2. Data Protection Officer responsibilities

The DPO is responsible for:

(a) Advising the School and its staff of its obligations under GDPR;

(b) Monitoring compliance with this GDPR and other relevant data protection law, the Schools policies with respect to this, and monitoring training and audit activities related to GDPR compliance;

(c) To provide advice where requested on data protection impact assessments;

(d) To cooperate with and act as the contact point for the ICO;

(e) the data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3. Staff responsibilities

Staff members who process personal data about students, staff, applicants or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) All personal data is kept securely;

(b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;

(c) Personal data is kept in accordance with the Schools retention schedule.

(d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Governance Team;

(e) Any data protection breaches are swiftly brought to the attention of Senior Managers and in turn the Information Governance team;

If staff are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Business Manager and Senior Leadership Team.

4. Third-Party Data Processors

Where external companies are used to process personal data on behalf of the School, responsibility for the security and appropriate use of that data remains with the School.

Where a third-party data processor is used:

(a) A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;

(b) Reasonable steps must be taken that such security measures are in place;

(c) A data processing agreement/written contract laying out exactly what the school expects of the third party must be signed by both parties.

6. Contractors, Short-Term and Voluntary Staff

The School is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that

they are appropriately vetted for the data they will be processing. In addition managers should ensure that:

(a) Personal data collected or processed in the course of work undertaken for the School is kept secure and confidential;

(b) Personal data is returned to the School on completion of the work, including any copies that may have been made. Alternatively it is securely destroyed and the School receives notification this has taken place

(c) The School is made aware of any disclosures of personal data to any other organisation or person who is not a direct employee of the contractor;

(d) Personal data is neither stored nor processed outside the UK unless written consent to do so has been received from the School;

(e) All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

6. Data protection by design and default

Under GDPR, the School has an obligation to consider the impact on data privacy during all processing activities. There is an obligation to consider the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons.

This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.

Senior managers are responsible for ensuring there is a privacy culture within the school, ensuring policies and procedures are developed with Data Protection in mind.

Data protection by design requires you to ensure that you consider privacy and data protection issues at the design phase of any system, service, product or process.

Data protection by default ensures you only process data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

7. Data Protection Impact Assessment

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted.

The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection requirements are not an after-thought.

You should conduct a DPIA (and discuss your findings with the DPO) in the following circumstances:

1. The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

2. Automated processing including profiling;

3. Large scale processing of sensitive (special category) data; and

4. Large scale, systematic monitoring of a publicly accessible area.

DPIA templates are provided by the Information Governance team and included the following; a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate; an assessment of the necessity and proportionality of the processing in relation to its purpose; an assessment of the risk to individuals; the mitigating measures in place and how we demonstrate compliance.

8. Rights of the data subject

GDPR was designed to strengthen the privacy rights of individuals. It offers more control to the data subject over what happens to their personal data, this has been expressed in GDPR under the following eight rights:

The Right to be informed

The right to be informed covers some of the key transparency requirements of GDPR, namely the first principle which promotes fair and transparent processing of personal data. Essentially, it' is about being as clear and concise as possible with the data subject and inform them how and why their information is being used.

Data subjects have the right to receive a copy of their personal data which is held by the School. In addition, an individual is entitled to receive further information about the Schools processing of their personal data as follows:

1. The purposes

2. The categories of personal data being processed

3. recipients/categories of recipient

4. Retention periods

5. Information about their rights

6. The right to complain to the ICO

7. Details of the relevant safeguards where personal data is transferred outside the EEA

8. Any third-party source of the personal data

The Right of Access

The right of access, commonly referred to as subject access, essentially gives individuals the right to obtain a copy of all their personal information. It helps individuals to understand how and why you are using their data, and also to check you are doing so lawfully.

The Right to Rectification

The right to rectification allows an individual to have any inaccurate information rectified. An individual may also be able to have incomplete personal data completed, although this depends on the purposes for the processing. This is closely linked to the 'Accuracy' principle of GDPR, however, although steps may have been taken to ensure that personal data was accurate when you obtained it, this right requires reconsideration of the accuracy upon request.

The Right to Erasure

The right to erasure, commonly referred to as, 'the right to be forgotten', gives individuals the right to have their personal data erased. However, this is not an absolute right and only applies in certain circumstances. A few examples of instances where it could apply would be:

I. If the personal data is no longer necessary for the purpose for which it was originally collected;
II. If 'consent' is the lawful basis for holding the data, and the individual withdraws their consent; and
III. You have processed the personal data unlawfully.

The Right to Restrict Processing

This right allows an individual to restrict the processing of their data. This means they can limit the way an organisation uses their data, and can be thought of as an alternative to

requesting the erasure. Similarly, this can only be applied in certain circumstances such as:

I. When the individual contests the accuracy of their personal data and you are in the process of verifying this accuracy;
II. The data has been processed unlawfully, and instead of erasure, the individual request restriction instead; and
III. You no longer need the personal data, but the individual requests you keep it in order to establish, exercise or defend a legal claim.

The Right to Data Portability

The right to data portability gives individuals the right to have any data they have provided to a controller to be moved between data controllers. This right only applies when the lawful basis for processing the information is either consent or for the performance of a contract. It also only applies to processing carried out digitally (i.e. this excludes paper files). The definition of 'provided to a controller' doesn't just mean direct information given to the controller, it can also mean personal data resulting from observation of an individual's activities.

This may include:

I. History of website usage or search activities;
II. Traffic and location data; or
III. 'Raw' data processed by connected objects such as smart meters and wearable devices.

The Right to Object

This gives individuals the right to object to the processing of their personal data, effectively asking the organisation to stop processing it. Again, this can only be used in certain circumstances and depends on the purposes and lawful basis used for processing.

An example of when this right can be applied is when:

Personal data is being used for direct marketing purposes and the individual wishes to object to this.

However, this right isn't absolute and will need to be carefully weighed up between the organisations' justification for processing the information, and the rights and freedoms of the individual.

The Rights to Automated Decision Making

GDPR has provisions on decisions which are made solely by automated means without any human involvement, and profiling (automated processing of data to evaluate certain things about an individual).

Examples of this would be:

I. An online decision to award a loan.
II. Or a recruitment aptitude test which uses pre-programmed algorithms and criteria.

GDPR restricts you from making solely automated decisions, included those based on profiling, that have a legal or similarly significant effect on an individual. The type of effect isn't specifically defined in GDPR however the decision must have a serious negative impact on an individual to be under the remit of this provision.

Heaton School has an individual Data Subject Rights policy – more information can be found here S:\HeadDocs\governors\governing body policies\resources policies\Policies 2018-19

9. Data Protection Breaches

Heaton School is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The School is required to make every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any suspected data protection incident must be brought to the attention of the Schools Information Governance Team who will investigate and decide if the incident constitutes a data protection breach.

If a reportable data protection breach occurs, the school is required to notify the ICO as soon as possible, and no later than 72 hours after becoming aware of it. Any member of the school who encounters something they believe may be a data protection incident must report it immediately.

More information can be found here S:\HeadDocs\governors\governing body policies\resources policies\Policies 2018-19

10. Consent

GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement between the school, parents and pupils.

GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Heaton School will keep clear records to demonstrate where consent has been given.

Heaton School has further information on the use of consent which can be found here S:\HeadDocs\governors\governing body policies\resources policies\Policies 2018-19

11. CCTV and photography

Heaton School currently as no CCTV.

12. Data sharing

Some bodies have a statutory power to obtain information such as regulatory bodies Health & Care Professions Council, the Nursing and Midwifery Council, Government agencies such as the Child Support Agency. You should seek confirmation of any such power before disclosing personal data in response to a request.

If the Police do not have a warrant they have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police to this effect.

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between the school and the third party must be signed, unless disclosure is required by law, such as certain requests from the Department for Education or the third party requires the data for law enforcement purposes.

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the students.

13. Record Keeping

The School is required to keep full and accurate records of all our data processing activities. We must keep and maintain accurate records reflecting our processing, including records of data subjects' consents and procedures for obtaining consents, where consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of the School as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. For our school this is captured within the Record of Processing Activity (RoPA).

Records of personal data breaches must also be kept, setting out:

1. The facts surrounding the breach

2. Its effects; and

3. The remedial action taken

Whilst record keeping is important, we must ensure that records are not kept for longer than necessary, they are retained and processed in line with the retention schedule and are securely destroyed once no longer needed.

14. Glossary of Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Data subjects for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data is data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behavior.

Data controller means the person/business who determines the purposes for which personal data will be processed, and the manner in which it will be processed.

Data processor means the person/business that processes personal data on behalf, and in accordance with the instructions, of a data controller.

Special category data includes information about a person's race, ethnic origin, political opinions, religion, trade union membership, genetics, Biometrics (where used for ID), health, sexual life, or Sexual orientation.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data Protection Officer (DPO): the person appointed as such under GDPR. A DPO is responsible for advising the School on their obligations under Data Protection, for monitoring compliance with data protection law, as well as with the Schools polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with GDPR.