Data Protection Policy

Heathcote School and Science College

Approved by:	Governors	**Date:** 16th January 2023
Last reviewed on:	Autumn 2021	
Next review due by:	Autumn 2026	

Other Documentation

This Policy should be used in reference with the following documents;

- E-Safety Policy
- Safeguarding Policy

Contents

Introduction

Heathcote School uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The school has a legal responsibility to comply with data protection legislation and other statutory provisions relating to the way in which is holds and processes personal data. The school, as a corporate body, is named as the Data Controller under the Act.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information is included in a public register which is available on the Information Commissioner's website at:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff, member of the governing board, contractors, and partners of the School that hold its' personal information has to comply with the law when managing that information. Schools also have a duty to issue a Privacy Notice to all pupils/parents and its' employees; these provide details of information collection and held, why it is held and the other parties to whom it may be passed on.

As data controller personal data collected about staff, pupils, parents, governors, visitors and other individuals that is collected and held must be processed in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the **UK General Data Protection Regulation**. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Scope of the Policy

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the school. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Under the **UK GDPR**, personal data' means any information relating to an identified or identifiable natural person ('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.

This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition,

it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

Definitions of data protection terms

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 controllers: are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Processors: include any person or organisation that is not a data user who processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our Schools behalf.

Data Protection Officer (DPO): is responsible for monitoring our compliance with data protection law.

Data Subject: ***means a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.***

Data users: are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Personal Data: ***means any information relating to an identified or identifiable natural person (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: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Processing: ***is any activity which is performed on personal data such as collection, recording, organisation, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.***

Special Category Personal Data: ***includes information about a person's racial or ethnic origin, political opinions; religious or philosophical beliefs; Trade Union membership; physical or mental health or condition; genetic/biometric data held for purposes of identification or data about sexual orientation or an individual's sex life.***

Roles and Responsibilities

This policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present pupils, employees, workers, or supplier contacts, website users or any other Data Subject.

Staff and those working on our behalf

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf.

You must read, understand and comply when Processing Personal Data on our behalf and attend training on its requirements. This policy sets out what we expect from you in order for the School to comply with applicable law. Your compliance with this policy is mandatory. You must also comply with all related Policies and guidelines given. Staff who do not comply with this policy may face disciplinary action.

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Ensuring that personal data held is accurate and up to date
- Ensuring that personal data held is not misused, lost or unlawfully disclosed

All staff must contact the DPO in the following circumstances:

- Where they are unsure or have questions about the operation of this policy; the purposes for which data may be used; retaining personal data; disclosing personal data or keeping personal data secure
- Where they are unsure if they have a lawful basis for processing personal data or wish to process for a different purpose than the one that the data was obtained
- Where they propose to engage in any activity that affects the rights of privacy of any individual i.e. where there is a legal obligation to carry out a Privacy Impact Assessment
- Where they are unsure about what security or other measures they need to implement to protect Personal Data
- If they need any assistance dealing with any rights invoked by a Data Subject
- Where they are considering sharing personal data with third parties
- Where they are entering into contracts involving the processing of personal data by another organisation

Where staff have concerns that this policy is not being followed by others they should report this immediately to the DPO. Where they wish to raise this formally they may do so under the **Schools' Policy and Procedure for reporting of Data Protection Infringements by Employees.**

Governing Board

The governing board or Governing Body has overall responsibility for ensuring compliance with all relevant data protection obligations.

Headteacher

The Headteacher has overall operational responsibility on a day-to-day basis for the implementation of the school's policies and procedures.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also a point of contact for individuals whose data the school processes who wish to raise any complaint regarding the school's processing where they remain dissatisfied with the school's response, and for the ICO.

Personal Data Protection Principles

We adhere to the principles relating to Processing of Personal Data set out in the **UK GDPR** which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

The school is committed to maintaining the data protection principles at all times. This means that the school will:

- Inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so

- Set out clear procedures for responding to requests for access to personal information known as subject access request
- Train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures

Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The **UK GDPR** restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The **UK GDPR** allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;
(b) the Processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations.;
(d) to protect the Data Subject's vital interests;
(e) the data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions - this is known as the Public Task
(f) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the **UK GDPR** and Data Protection Act 2018.
If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

The purposes for which we process Personal Data to perform our Public Task are set out in the Privacy Notice issued by the School.

When we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we provide the Data Subject with all the information required by the **UK GDPR** including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing (Privacy) Notice.

Sharing Personal Data

The School will not normally share personal data with anyone else without express consent, but may do so where:

- It is necessary for the performance of our Public Task
- There is an issue with a pupil or parent/carer that puts the safety of another individual at risk
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we:
  (i) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

(ii) Establish either in the contract or as a standalone agreement, a data processing agreement to ensure the fair and lawful processing of any personal data we share
(iii) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for the following purposes:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.
We may enter into Information Specific Sharing Agreements with other public bodies for the purposes outlined above.

Subject Access Requests and Other Rights of Individuals

Our Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;
(b) receive certain information about how we process their data;
(c) request access to their Personal Data that we hold;
(d) prevent use of their Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
(f) restrict Processing in specific circumstances;
(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) object to decisions based solely on Automated Processing, including profiling (known as Automated Decision Making ADM);
(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(l) make a complaint to the Information Commissioner; and
(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Where an individual exercises their rights of subject access this will be dealt with under the schools **Subject Access Request Policy and Procedure**.

Parents, or those with parental responsibility, have a legal right to access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system, pupils use pin numbers to receive school dinners instead of paying with cash, parents/carers have been notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent before we take any biometric data and first process it.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Julie Vazquez, School Business Director.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding policy and E Safety Policy for more information on our use of photographs and videos.

Record Keeping

The **UK GDPR** requires us to keep full and accurate records of all our data Processing activities.

We keep and maintain accurate records reflecting our Processing. These records include 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.

Accountability, Data Protection by Design

We put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment, (see our ICT Acceptable Use policy.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.
In the unlikely event of a suspected data breach, we will follow the Schools Personal Data Breach Procedure and take all steps we can to remedy the breach that has occurred.
When appropriate, we will report the data breach to the ICO within 72 hours.

Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Review and Monitoring Arrangements

This policy will be reviewed and updated as and when necessary. The DPO will review this policy at every annual audit and report any necessary changes to the governing board.
Further specialist information and advice may be sought from the Schools Data Protection Officer (see details below)
For help or advice on this policy please contact:

Maryline Alvis
Education Data Protection Officer via

Education Data Protection Service Team
Governance & Law
London Borough of Waltham Forest
Email: edposervice@walthamforest.gov.uk

Or

Julie Vazquez
Data Protection Officer for Heathcote School