THE HOWARD
Academy Trust

# Data Protection/GDPR Policy

Date of last review: September 2025

## Document Management Information

| | |
|---|---|
| **Applicable to:** | All staff in all Academies and Central Support Services including individuals employed by the Trust and agency staff.<br><br>All Members and Trustees. |
| **Dissemination:** | The policy will be available to staff via the Trust's Policy Centre and website |
| **Training:** | On request |
| **Review frequency:** | The policy will be reviewed biennially. The policy will be reviewed earlier if needed in the light of new evidence, legislation and guidance |
| **Policy Author:** | Cathy Reid – Deputy CEO |
| **Executive Policy Owner:** | Owen McColgan – Chief Executive |
| **Approval by:** | Level 3 – Chief Executive Approval |
| **Approval date:** | September 2025 |
| **Next review date:** | July 2027 |

## Revision History

| Document Version | Description of Revision | Date Approved |
|---|---|---|
| V1.0 | Policy approved by CEO | September 2021 |
| **V1.2** | Updates to document management information | September 2025 |
| | | |

THE HOWARD
Academy Trust

## Contents

# DATA PROTECTION/GDPR Policy

## Policy Statement

The Howard Academy Trust and its member academies are committed to meeting their legal obligations concerning data protection. The Trust has due regard for everyone's rights when handling personal data during the course of its activities. They will collect, store and process personal information about students, students' families, staff, volunteers, contractors, suppliers and other third parties pupils and may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other academies and educational bodies, and potentially Social Services in accordance with its legal obligations in accordance with its legal obligations under the General Data Protection Regulation (GDPR), the core principles of which are:

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security)
- Accountability.

General information about the Data Protection Act and GDPR can be obtained from the Information Commissioner's Office (Help Line 0303 123 1113, website www.ico.org.uk).

### Data Protection Officer (DPO)

**The Howard Academy Trust's Data Protection Lead is:**

**Trust Data Manager**
**The Howard Academy Trust**
**C/O Waterfront UTC**
**South Side Three Road**
**Chatham**
**Kent**

**Email: dpo@thatrust.org.uk**

THAT also use an external Data Protection Officer – School Pro.
They can be contacted by emailing dpo@schoolpro.co.uk

The DPO will:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's 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.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to academies.

The DPO will report to the highest level of management at the Trust, which is the Chief Executive.

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.

## Legal framework

This policy has due regard to legislation including, but not limited to, the following:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Academy Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

This policy will be implemented in conjunction with the following other academy policies:

- Use of Videos and Photographs at School Events
- E-Safety Policy
- Freedom of Information Policy
- CCTV Policy
- Cloud Storage Policy. The Howard Academy Trust currently stores financial data via a secure cloud-based system.

### Responsibilities

The Local Academy Board have overall responsibility for the compliance with the Data Protection Act (DPA/General Data Protection Regulations (GDPR) within their academy. The Principal is responsible for ensuring compliance with the DPA/GDPR and this policy within the day to day activities of the academy. The Headteacher/Principal is responsible for ensuring appropriate training is provided for all staff. The policy will be evaluated by the Finance, Audit & Resources Committee every two years.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA/GDPR and must ensure that personal information is kept and processed in line with the DPA/GDPR.

## Fair Obtaining and Processing

The Howard Academy Trust undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

**"processing"** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

**"data subject"** means an individual who is the subject of personal data or the person to whom the information relates.

**"personal data"** means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, as can names and photographs should they be published or displayed in the press, Internet or media.

**"parent/carer"** has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

## Data Integrity

The academy undertakes to ensure data integrity by the following methods:

## Data Accuracy

*If data subjects inform the Academy of any change of circumstances, their record shall be updated accordingly on any system or any form their data is held.*

Where a data subject challenges the accuracy of their data, the Trust/academy will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, there will be an attempt to resolve the issue informally but, if this proves impossible, disputes will be referred to the Local Academy Board for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved, the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information. More information regarding correcting inaccurate or incomplete data is detailed on page 11.

## Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the academy will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

## Authorised Disclosures

The Trust and academies will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the academy's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the academy to perform its statutory duties and obligations.

- Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.

- Student data disclosed to parent/carers in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the academy.

- Staff data disclosed to relevant authorities, eg in respect of payroll and administrative matters related to employment.

- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances, the engineer would be required to sign a form promising not to disclose the data outside the academy.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the academy by administrative staff, teachers and others will only be made available where the person requesting the information is a professional legitimately working within the academy who **needs to know** the information in order to do their work. The academy will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that might suggest that the student is, or has been, the subject of, or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the academy, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the academy's registered purposes.

## Data and Computer Security

The Trust and academies undertake to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

## Physical Security

Appropriate building security measures are in place, such as alarms and locks. Only authorised persons are allowed in the admin and IT offices. Disks, tapes and printouts are locked away securely when not in use. Visitors to Trust sites are required to sign in and out, to wear identification badges and are, where appropriate, accompanied.

## Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes regularly taken place. Computer files are backed up (ie security copies are taken) regularly.

## Procedural Security

In order to be given authorised access to the computer system, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall, the policy for data is determined by the Local Academy Board and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the academy should, in the first instance, be referred to the academy's main office.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter and serious breaches could lead to dismissal.

## Applicable Data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier/IP address. The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, eg key-coded.

**Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

## Principles

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

- 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. 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.
- 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. Every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- 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 the GDPR in order to safeguard the rights and freedoms of individuals.
- 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 GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

## Accountability

The Trust and academies will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The academies will provide comprehensive, clear and transparent privacy policies.

Additional internal records of the academy's processing activities will be maintained and kept up-to-date.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

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

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

Data protection impact assessments will be used, where appropriate.

## Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:

— Compliance with a legal obligation.
— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
— For the performance of a contract with the data subject or to take steps to enter into a contract.
— Protecting the vital interests of a data subject or another person.
— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent, is prohibited by EU or Member State law.

- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

## Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

Academies ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR. However, acceptable consent obtained under the DPA will not be reobtained. Consent can be withdrawn by the individual at any time.

The consent of parents/carers will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

## The Right to be Informed

The privacy notice supplied to individuals with regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the academy will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

## The Right of Access

Appropriate measures have taken to provide information referred to in GDPR regulations Articles 13 and 14 in and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (ie verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request was received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in

exceptional circumstances and the data subject is kept informed in wiring throughout the retrieval process of any delays or reasons for delay.

Where the Trust/academy does not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

## Subject Access Request (SAR)

Where a data subject asks us to confirm whether personal data concerning them is held and processed and requests access to such data; they will be provided with:

- The purposes of the processing;
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- The right to lodge a complaint with a Supervisory Authority;
- Where personal data has not been collected by THAT or the academy from the data subject, any available information as to the source and provider;
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

SARs are passed to the Data Protection Lead as soon as received and a record of the request is noted. Given that personal data is to be disclosed, a verification of identity (document with the data subject's name and address, email, etc.) should be completed. If the requestor is entitled to the personal data, the request can be processed. The type of personal data held about the individual is checked against the Information Inventory to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

**SARs are completed within 30-days and are provided free of charge**. Where the individual makes the request by electronic means, the information will be provided in a commonly used electronic format, unless an alternative format is requested.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the academy will ask the individual to specify the information the request is in relation to.

### Data Portability

The Trust and its academies provide all personal information pertaining to the data subject, to them on request and in a format that is easy to disclose and read. Compliance with the data portability rights of individuals will ensure that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

Where requested by a data subject for whom consent to process and share their personal information is held and when processing is carried out by automated means, personal data will be transmitted directly to a designated controller, where technically feasible. To ensure compliance with Article 20 of the GDPR concerning data portability, a machine-readable version of all personal information will be kept utilising the below formats for compliance:

- .DOC;
- .XLS;
- PDF;
- JPG/image;
- Unicode (outlook email).

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, the request is not responded to, a full, written explanation within 30 days will be provided to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

### Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by THAT/the academy is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform the Trust/academy that the data held is inaccurate, every reasonable step will be taken to ensure that such inaccuracies are corrected with immediate effect.

Where notified of inaccurate data by the data subject, the error will be rectified within 30 days and any third party will be informed of the rectification if the personal data in question has been disclosed to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

Where notified of incomplete data, the information will be completed as directed by the data subject, including adding an addendum or supplementary statement where applicable. If for any reason, the Trust/academy are unable to act in response to a request for rectification and/or completion, a written explanation to the individual will always be provided and they will be informed of their right to complain to the Supervisory Authority and to a judicial remedy.

## The Right to Erasure

Also, known as 'The Right to be Forgotten', The Howard Academy Trust complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed. All

personal data obtained and processed by The Howard Academy Trust is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable compliance with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst standard procedures already remove data that is no longer necessary, a dedicated process for erasure requests is still followed to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where a request to erase and/or remove personal information from a data subject is received, the process below is followed:

The request is allocated to the Data Protection Lead and Trust Executive are informed once the identity has been confirmed and recorded.

↓

The Data Protection Lead locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended.

↓

The request is reviewed to ensure it complies with one or more of the grounds for erasure:

a) The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
b) The data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing;
c) The data subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) The personal data has been unlawfully processed;
e) The personal data must be erased for compliance with a legal obligation;
f) The personal data has been collected in relation to the offer of information society services to a child.

↓

If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received.

↓

The Data Protection Lead writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure.

↓

Where The Howard Academy Trust/academy has made any of the personal data public and erasure is granted, every reasonable step and measure will be taken to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data.

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. If for any reason, the Trust/academy are unable to act in response to a request for erasure, a written explanation to the individual will be provided and they will be informed of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include:

- Exercising the right of freedom of expression and information;
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- For the establishment, exercise or defence of legal claims.

## The Right to Restrict Processing

There are certain circumstances where The Howard Academy Trust restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subject's request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Howard Academy Trust will apply restrictions to data processing in the following circumstances:

- Where an individual contests the accuracy of the personal data and the process of verification has not been completed and/ corrections made;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and consideration is taking place as to whether there are legitimate grounds to override those of the individual;
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure;
- Where the personal data is no longer needed, but the data subject requires the data to establish, exercise or defend a legal claim.

The Data Protection Lead reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and such data to a third-party has been disclosed, the third-party will be informed of the restriction in place and the reason and will be re-informed if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. The data subject is provided in writing of any decision to lift a restriction on processing. If for any reason, the Trust/academy are unable to act in response to a request for restriction, a written explanation to the individual will always be provided and they

will be informed their right to complain to the Supervisory Authority and to a judicial remedy.

## Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in the Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. Opt-out options will be provided on all direct marketing material and an online objection form where processing is carried out online. Individuals have the right to object to:

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics.

Where The Howard Academy Trust and its academies process personal data for the performance of a legal task, in relation to their legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on 'grounds relating to their particular situation'. The Trust/academy reserves the right to continue processing such personal data where:

- They can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- The processing is for the establishment, exercise or defence of legal claims.

Where personal information for direct marketing purposes under a previously obtained consent are processed, processing such personal data will be stopped immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the processing will cease for that purpose and the data subject will be advised of the cessation in writing within 30 days of the objection being received.

The Trust understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the GDPR, aim to put measures into place to safeguard individuals where appropriate. Via the Privacy Notices, in first communications with an individual and on Trust and academy websites, individuals are advised of their rights not to be subject to a decision when:

- It is based on automated processing;
- It produces a legal effect or a similarly significant effect on the individual.

In no circumstances does The Howard Academy Trust and its academies use automated decision-making processes.

## Privacy by Design and Privacy Impact Assessments

The Trust and academies will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the academy has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the academy's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the academy's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:
- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The academy will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the academy will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

## Data Breaches

The term '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. The Headteacher/Principal will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the academy becoming aware of it. The supervisory authority in the first instance will be the Director of Finance & HR at the Trust.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the academy will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

## Data Security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for academy purposes.
All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises either in electronic or paper format, staff will take extra care to follow the same procedures for security, eg keeping devices under lock and key. The person taking the information from the academy premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the academy containing sensitive information are supervised at all times.
- The physical security of the academy's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Headteacher/Principal is responsible for continuity and recovery measures are in place to ensure the security of protected data.

## Publication of Information

The academy publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

## CCTV and Photography

The academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The academy notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes. The Headteacher/Principal is responsible for keeping the records secure and allowing access.

The academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the academy wishes to use images/video footage of pupils in a publication such as the academy website, prospectus, or recordings of academy plays, written permission will be sought for the particular usage from the parent of the pupil.

Precautions, as outlined in the Photography and Videos at Academy Policy, are taken when publishing photographs of pupils, in print, video or on the academy website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## Data Retention Period

*'In accordance with Article 5(1)(e) of the GDPR,data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Trust/academy to ensure that obsolete data is properly erased.*

Some educational records relating to former pupils or employees of the academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

## DBS Data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Please refer to the Trust-wide DBS Policy.

## Biometric Data

The Trust operates a biometric recognition system for purposes such as dinner money payments and secure entry systems.
Consent must be obtained in accordance with the Protection of Freedoms Act 2012.
Alternative access methods must be provided if consent is not given.

## Complaints Procedure

A Complaints will be acknowledged within 30 days.
An investigation will be conducted in accordance with the Trust Complaints Procedure

## Data Processors

Due diligence will be conducted before engaging data processors.
Contracts will include obligations for data protection compliance.
Processors must adhere to the Trust's data protection standards.

## Remote Working Practices

Staff must use secure networks and avoid unsecured USB devices.
Home environments must be safeguarded to protect personal data.
Remote working practices must comply with the Trust's data protection policy.

## Automated Decision-Making

Individuals have the right to object to automated decisions.
The Trust does not currently use automated decision-making systems.

## Reference to the Data (Use and Access) Act 2025

This policy anticipates changes due to the Data (Use and Access) Act 2025 and will be updated accordingly.

## Policy Review

The policy will be monitored by the Data Protection Officers and evaluated by the Finance, Audit and Resources Committee every two years.

## Monitoring and Evaluation

Data Protection/GDPR Policy will be monitored by Local Academy Boards and evaluated by the Finance, Audit and Resources Committee.

## Definitions Annex

- Personal Data: Any information relating to an identified or identifiable individual.
- Data Controller: The entity that determines the purposes and means of processing personal data.
- Data Processor: An entity that processes personal data on behalf of the controller.
- Biometric Data: Personal data resulting from specific technical processing relating to physical, physiological or behavioral characteristics.