



# **Data Protection and Freedom of Information Policy**

## **1. INTRODUCTION.**

The Hazeley Academy (The Academy) collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Academy in order to provide education and associated functions.

The Academy may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

The academy informs individuals of the type of data we process and what we do with this information through our privacy notices that can be found here:

<http://www.thehazeleyacademy.com/welcome/policies/>

The GDPR apply to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use an individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation and shall be reviewed every 2 years.

## **2. PERSONAL DATA.**

Personal data is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain.

A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

- ✓ Race or ethnic origin
- ✓ Political opinions
- ✓ Religious or philosophical beliefs
- ✓ Trade union membership
- ✓ Physical or mental health
- ✓ An individual's sex life or sexual orientation
- ✓ Genetic or biometric data for the purpose of uniquely identifying a natural person

Special Category Information is given special protection and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The Academy does not intend to seek or hold sensitive personal data about staff or students except where the Academy has been notified of the information, or it comes to the Academy's attention via legitimate means e.g. a grievance or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Academy their race or ethnic origin, political or religious beliefs, whether or not they are a trade

union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

The Academy is the data controller for the purposes of the [Data Protection act 2018](#) and is registered with the [Information Commissioner's Office](#)

Personal data should always be kept securely and protected by passwords if it is electronic; access should only be those authorised to see it – confidentiality should be respected. The law also provides that personal data should not be kept longer than is required.

### **3. THE DATA PROTECTION PRINCIPLES.**

The six data protection principles as laid down in the GDPR are followed at all times:

- ✓ Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met.
- ✓ Personal data shall be collected for specific, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.
- ✓ Personal data shall be adequate, relevant and limited to what is necessary for the purpose for which it is being processed.
- ✓ Personal data shall be accurate and where necessary, kept up to date.
- ✓ Personal data processed for any purpose (s) shall not be kept for longer than is necessary for that purpose / those purposes.
- ✓ Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition to this, the Academy is committed to ensuring at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law

The Academy is committed to complying with the principles (3.1) at all times. This means the Academy will:

- ✓ Inform individuals as to the purpose of collecting any information from them, as and when we ask for it.
- ✓ Be responsible for checking the quality and accuracy of the information.
- ✓ Regularly review the record held to ensure that information is not held longer than is necessary and that it has been held in accordance with statutory and best practice for data retention
- ✓ Ensure that when information is authorised for disposal it is done appropriately.
- ✓ Ensure appropriate security measures to safe guard personal information whether it is held in paper files or on our computer systems
- ✓ Share personal information with others only 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 requests.
- ✓ Report any breaches of the GDPR in accordance with procedures stated in section 12.

#### **4. CONDITIONS FOR THE PROCESSING IN THE FIRST DATA PRINCIPLE.**

One or more of the following conditions must be met in order to process data. A register of processing activities and conditions met will be maintained by the Academy along with an asset register of the systems used.

- ✓ The individual has given consent that is specific to the particular type of processing activity and that consent is informed, unambiguous and freely given.
- ✓ The process is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual at their request.
- ✓ The processing is necessary for the performance of a legal obligation to which we are subject.
- ✓ The processing is necessary to protect the vital interests of the individual or another.
- ✓ The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.
- ✓ The processing is necessary for a legitimate interest of the School or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

#### **5. USE OF PERSONAL DATA BY THE SCHOOL.**

The Academy holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in Section 3.

##### **Pupils**

The personal data held regarding pupils includes, but is not limited to, contact details, assessment, examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information and photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care and to assess how well the Academy as a whole is doing, together with any other uses normally associated with this provision in a school environment.

In particular, the Academy may:

- ✓ Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities.
- ✓ Keep the pupil's previous school informed of his/her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the School to the previous school.
- ✓ Use of photographs of pupils in accordance with the photograph policy.

##### **Staff**

The personal data held about staff will include, but is not limited to, contact details, employment history, information relating to their career progression, information relating to DBS checks, photographs, training records, emergency contact details, sickness records including medical certificates.

The data is used to comply with legal obligations placed on the School in relation to employment and the education of Children in a school environment.

The Academy may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

Staff should note that information about disciplinary action may be kept longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

### **Other Individuals**

The Academy may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

### **Right to limit or object**

Any wish to limit or object to the uses to which personal data is to be put should be notified to the Data Lead, Stephen Whitney (MSW), who will ensure that it is recorded and adhered to if appropriate. If the Data Lead is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Academy cannot comply with their request.

## **6. SECURITY OF PERSONAL DATA.**

The Academy will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR.

The Academy will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

For further details as regards security of IT systems, please refer to the ICT policy

## **7. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES.**

The following list includes the most usual reasons that the Academy will authorise disclosure of personal data to a third party:

- ✓ To give a confidential reference relating to a current or former employee, volunteer or pupil.
- ✓ For the prevention or detection of crime.
- ✓ For the assessment of any tax or duty.
- ✓ Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Academy (other than an obligation by contract).
- ✓ For the purpose of, or in connection with legal proceedings (including prospective legal proceedings).
- ✓ For the purpose of obtaining legal advice.
- ✓ For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress).
- ✓ To publish the results of public examinations or other achievements of pupils of the Academy.
- ✓ To disclose details of a pupil’s medical condition where it is in the pupil’s interests to do so, for example for medical advice, insurance purposes or to organisers of school trips.
- ✓ To provide information to another educational establishment to which a pupil is transferring

- ✓ To provide information to the Examination Authority as part of the examination process: and
- ✓ To provide information to the relevant Government Department concerned with national education. At the time of writing this policy this department is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

The Academy may receive requests from third parties (i.e. those other than the data subject, The Academy and employees of the Academy) to disclose personal data it holds about pupils, their guardians or parents, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosures apply, or where necessary for the legitimate interests of the Academy.

All requests for the disclosure of personal data must be sent to the Data Lead (MSW) who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third person before making any disclosure.

## **8. CONFIDENTIALITY OF PUPIL CONCERNS.**

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Academy will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent or where the School believes disclosure will be in the best interests of the pupil or other pupils.

Child protection and safeguarding take precedence in all areas around confidentiality of pupil concerns

## **9. SUBJECT ACCESS REQUESTS.**

Anybody who makes a request to see any personal information held about them by the Academy is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system." (Section 1)

All request should be sent to DPL within 3 working days of receipt and must be dealt with without delay and at the latest within one month of receipt.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under 12, or over 12 with special educational need which make understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. XXX must however be satisfied that: -

- ✓ The child or young person lacks sufficient understanding and
- ✓ The request made on behalf of the child or young person is in their interests.

Any individual including a child or young person with ownership of their own information rights, may appoint another person to request access to their records.

In such circumstances the Academy must have written evidence that the individual has authorised the person to make the application and XXX must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A subject access request must be made in writing. The Academy may ask for any further information reasonably required to locate the information.

An individual only has the automatic right to access information about themselves and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by XXX before any disclosure takes place. Access will not be granted before this review has taken place.

Where the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

## **10. EXEMPTIONS TO ACCESS BY DATA SUBJECTS**

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.

## **11. OTHER RIGHTS OF INDIVIDUALS.**

The Academy has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following section sets how the Academy will comply with the rights to:

- ✓ Object to Processing.
- ✓ Rectification.
- ✓ Erasure.
- ✓ Data.

### **Right to object to processing.**

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

Where such an objection is made, it must be sent to the Data Lead within 2 working days of receipt and in consultation with the Data Protection Officer will assess whether there are compelling legitimate grounds to continue processing which override the interest, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The Data Lead shall be responsible for notifying the individual of the outcome of their assessment within 10 working days of receipt of the objection.

### **Right to rectification.**

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Data Lead within 2 working days of receipt and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable and the individuals notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of either a review by the Data Protection Officer or an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data and any information submitted in this way shall be updated without undue delay.

### **Right to erasure.**

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arise in the following circumstances.

- ✓ Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed.
- ✓ Where consent is withdrawn and there is no longer other legal basis for the processing.
- ✓ Where an objection has been raised under the “Right to Object” and found to be legitimate.
- ✓ Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met).
- ✓ Where there is a legal obligation on the Academy to delete.

The Data Lead will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data and this data has been passed to other data controllers and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

### **Rights to restrict processing**

In the following circumstances, processing of an individual’s personal data may be restricted:

- ✓ Where the accuracy of data has been contested, during the period when the Academy is attempting to verify the accuracy of the data.
- ✓ Where processing has been found to be unlawful and the individual has asked that there be a restriction on processing rather than erasure.
- ✓ Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim.
- ✓ Where there has been an objection made under the Right to Object pending the outcome of any decision.

### **Right to portability.**

If an individual wants to send their data to another organisation they have a right to request that the Academy provides their information in a structured, commonly used and machine readable format. As this right is limited to situations where the Academy is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the Data Lead within 2 working days of receipt and they will review and process as necessary.

### **Personal electronic devices and CCTV**

Where necessary for the execution of its responsibilities under legislation the academy may obtain data from personal electronic devices. The member of staff obtaining the data will ensure that they explain the reasons why they are taking the data and that it will be stored securely in a limited and protected area. Access will be limited to those who need it in order to fulfil their roles and responsibilities and storage and disposal will occur as per the rest of the policy. Requests for access to this data are explained earlier in this policy. The academy reserves the right to use CCTV within its premises for the purpose of safety and crime prevention. Images will be stored on a secure server with limited and protected access for those who need it in order to fulfil their roles and responsibilities. Where this data is used for the purposes outlined above, storage and disposal will occur as per the rest of the policy

## **12. BREACH OF ANY REQUIREMENT OF THE GDPR.**

Any and all breaches of the GDPR, including a breach of any of the data protection principles, shall be reported as soon as it is discovered to the Data Protection Lead

Once notified, the Data Protection Lead will assess in conjunction with the Data Protection Officer

- ✓ The extent of the breach.
- ✓ The risks to the data subjects as a consequence of the breach.
- ✓ Any security measures in place that will protect the information.
- ✓ Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Data Protection Lead and Officer concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office with 72 hours of the breach having come to the attention of the Academy, unless a delay can be justified. The Information Commissioner shall be told:

- ✓ Details of the breach, including the volume of the data at risk and the number and categories of data subjects.
- ✓ The contact point for any enquiries (which will normally be the Data Protection Officer).
- ✓ The likely consequence of the breach.
- ✓ The measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals, then the Data Protection Lead shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- ✓ The nature of the breach.
- ✓ Who to contact with any questions.
- ✓ Measures taken to mitigate any risks.

The Data Protection Officer shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Academy and a decision made about implementations of this recommendations.

If the breach is not likely to present a risk to individuals, the same processes shall apply, but an internal record shall be kept instead.

### **13.CONTACT**

If anyone has any concerns or questions in relation to this Policy, they should contact the Data Protection Lead (MSW)

## **FREEDOM OF INFORMATION.**

### **1. Introduction**

The Academy is subject to the [Freedom of Information Act 2000 \(FOI\)](#) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

### **2. WHAT IS A REQUEST UNDER FOI**

Any request for information from the Academy is technically a request under the FOI, whether or not the individual making the request mention the FOI.

However, the ICO has stated that routine requests for information (such as parent requesting a copy of policy) can be dealt with outside of the provision of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescales set out below. A copy of the request and response should then be sent to the DPL

All other requests should be referred in the first instance to DPL who may allocate another individual to deal with the request. This must be done promptly and in any event within 3 working days of receiving the request.

When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information “confidential” or “restricted”.

### **3. TIME LIMIT FOR COMPLIANCE**

The Academy must respond as soon as possible and in any event, within 20 working days of the date of receipt of the request. For the Academy, when calculating the 20 working days deadline, a “working day” is a school day (one in which the pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days” to respond.

### **4. PROCEDURE FOR DEALING WITH A REQUEST**

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the DPL, who may re allocate to an individual with responsibility for the type of information requested.

The first stage in responding is to determine whether or not the Academy “holds” the information requested. The Academy will hold the information if it exists in computer or paper format. Some requests will require the Academy to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Academy is considered to “hold” that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Academy to add up the totals in a spreadsheet and release the total figures, this would be information “held” by the Academy. If the Academy would have to go through a number of spreadsheets and identify

individual figures and a provide a total, this is likely not to be information “held” by the Academy, depending on the time involved in extracting the information.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- ✓ Section 40 (1) – The request is for the applicant’s personal data. This must be dealt with the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy.
- ✓ Section 40 (2) – Compliance with the request would involve releasing third party data, and this would be in breach of the DPA principles as section 3 of the DP policy
- ✓ Section 41 – Information that has been sent to the Academy (but not the Academy’s own information) which is confidential.
- ✓ Section 21 – Information that is already publicly available, even if payment of a fee is required to access that information.
- ✓ Section 22 – Information that the Academy intends to publish at a future date.
- ✓ Section 43 – Information that would prejudice the commercial interests of the Academy and / or a third party.
- ✓ *Section 38 – Information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information).*
- ✓ *Section 31 – Information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras.*
- ✓ *Section 36 – Information which, in the opinion of the chair of governors of the School, would prejudice the effective conduct of the School. There is a special form for this on the ICO’s website to assist with the obtaining of the chair’s opinion.*

The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighing exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

## 5. **RESPONDING TO A REQUEST.**

When responding to a request where the Academy has withheld some or all of the information, the Academy must explain why the information has been withheld, quoting the appropriate section number and explaining how the information was requested fits with that exemption. If the public interest test has been applied, this also needs to be explained.

The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by (a governor), or by writing to the ICO.

## 6. CONTACT

Any questions about this policy should be directed in the first instance to the Data Protection Lead (MSW)