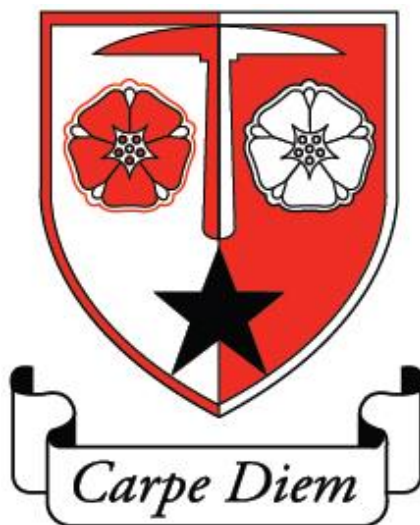


# Audenshaw School



## DATA PROTECTION POLICY

This policy is reviewed annually by the Personnel Committee.

### History of Document

Issue No	Author/Owner	Date Written	Approved by the Personnel Committee	Received by Governors	Comments
2	Sarah Monks	09/11/2020	09/12/2020	09/12/2020	Full review and minor amendments
2.1	Sarah Monks	11/01/2022	14/02/2022	14/02/2022	Minor amendments
2.2	Sarah Monks	28/04/2023	13/06/2023	13/06/2023	Minor amendments

## CONTENTS

		PAGE
1.	Aims	3
2.	Legislation and guidance	3
3.	Definitions	3
4.	The data controller	5
5.	Roles and Responsibilities	5
6.	Data Protection Principles	5
7.	Collecting personal data	6
8.	Sharing personal data	6
9.	Subject access requests and other rights of individuals	7
10.	Parental requests to see the educational record	9
11.	Biometric recognition systems	9
12.	CCTV	9
13.	Photographs and videos	9
14.	Data protection by design and default	10
15.	Data security and storage of records	10
16.	Disposal of records	11
17.	Personal data breaches	11
18.	Training	11
19.	Links with other policies	11
Appendix 1	Personal data breach procedure	12
Appendix 2	Subject access request	14

Appendix 3	Initial response to subject access request	15
Appendix 4	Subject access request (Parent)	16
Appendix 5	Reply to subject access request	17
Appendix 6	Privacy notice (Parent/carer)	18
Appendix 7	Privacy notice (Students)	22
Appendix 8	Privacy notice (Suppliers)	25
Appendix 9	Privacy notice (Visitors)	28
Appendix 10	Privacy notice (School workforce)	31
Appendix 11	Privacy notice (Governors and other volunteers)	34
Appendix 12	Privacy notice (Job applicants)	37

## 1. Aims

The School aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual.  This may include the individual's:

	<ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<b>Data controller</b>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<b>Data processor</b>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
<b>Personal data breach</b>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>

## 4. The data controller

The School processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and responsibilities

This policy applies to **all staff** employed by Audenshaw School, and to external organisations or individuals working on the school's behalf. Staff who do not comply with this policy may face disciplinary action.

### 5.1 Governing board

The governing board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

### 5.2 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 the first point of contact for individuals whose data the School processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The DPO is Mrs S Monks and is contactable via the contact form on the School website.

### 5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals to ask if a Data Protection Impact Assessment is necessary.
  - If they need help with any contracts or sharing personal data with third parties

## 6. Data protection principles

The GDPR is based on data protection principles that the School must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the School aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

The School will only process personal data where the School has one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract
- The data needs to be processed so that the School can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- 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
- The data needs to be processed for the **legitimate interests** of the School or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carers when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, the School will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If the School offer online services to students, such as classroom apps, and the School intend to rely on consent as a basis for processing, the School will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever the School first collect personal data directly from individuals, the School will provide them with the relevant information required by data protection law.

### 7.2 Limitation, minimisation and accuracy

The School will only collect personal data for specified, explicit and legitimate reasons. The School will explain these reasons to the individuals when the School first collect their data.

If the School want to use personal data for reasons other than those given when the School first obtained it, the School will inform the individuals concerned before the School do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's retention policy which is based on the guidance provided in the [Information and Records Management Society's toolkit for Schools](#).

## 8. Sharing personal data

The School will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carers that puts the safety of our staff at risk
- The School need to liaise with other agencies – the School will seek consent as necessary before doing this

The School's suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, the School will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the School share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the School

The School will also share personal data with law enforcement and government bodies where the School are legally required to do so, including for:

- The prevention or detection of crime and/or fraud. The School will only share students details to Police once a Police Data Disclosure form is received and authorised by a Senior Officer. The only exception to this is for Safeguarding reasons or if the school report a crime and need to give Police data to enable them to pursue this. All Police disclosure forms need to be authorised by the Data Controller.
- The apprehension or prosecution of offenders
- The assessment or collection of tax 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

The School may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of its students or staff.

Where the School transfer personal data to a country or territory outside the European Economic Area, the School will do so in accordance with data protection law.

## **9. Subject access requests and other rights of individuals**

### **9.1 Subject access requests (Appendices 2 & 3)**

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

## **9.2 Children and subject access requests (Appendix 4)**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at the School may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

## **9.3 Responding to subject access requests (Appendix 5)**

When responding to requests, the School:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual the School will comply within 3 months of receipt of the request, where a request is complex or numerous. The School will inform the individual of this within 1 month, and explain why the extension is necessary

The School will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the School may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When the School refuse a request, the School will tell the individual why, and tell them they have the right to complain to the ICO.

## **9.4 Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when the School are collecting their data about how the School use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)



Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 10. Parental requests to see the educational record

Under the principles of the General Data Protection Regulations 2018 (GDPR) and the Data Protection Act 2018 (the DPA 2018), children and young adults can assume control over their personal information and restrict access to it from the age of 13.

However, parents are entitled to request access to, or a copy of their child's educational record, even if the child does not wish them to access it. This applies until the child reaches the age of 18. A parent is not, however entitled to information that the School could not lawfully disclose to the child under the GDPR or in relation to which the child would have no right of access.

(<http://www.legislation.gov.uk/ukxi/2005/1437/regulation/5/made>). For any queries about GDPR the Information Commissioners Office (<http://ico.org.uk>) can be contacted.

## 11. Biometric recognition systems

Where the School use students' biometric data as part of an automated biometric recognition system (for example, students provide a numerical algorithm based on a unrecorded scan of the finger to receive School dinners instead of paying with cash the School will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be 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 from at least one parent or carer before the School take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the School's biometric system(s). The School will provide alternative means of accessing the relevant services for those students. For example, students can pay for School dinners using a pin number.

Parents/carers and students can object to participation in the School's biometric recognition system(s), or withdraw consent, at any time, and the School will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use the School's biometric system(s), the School 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.

## 12. CCTV

The School use CCTV in various locations around the School site to ensure it remains safe. The School will adhere to the ICO's [code of practice](#) for the use of CCTV.

The School do not need to ask individuals' permission to use CCTV, but the School 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 Mrs Monks, Head of Executive Services. In accordance with good practice, CCTV footage is deleted after 30 days

## 13. Photographs and videos

As part of the School activities, the School may take photographs and record images of individuals within the School.

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

Where the School need parental consent, the School will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where the School does not need parental consent, the School will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- 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, the School will delete the photograph or video and not distribute it further.

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

## **14. Data protection by design and default**

The School will put measures in place to show that the School have integrated data protection into all of the data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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 (see section 6)
- 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 (Appendices 6,7,8,9,10,11 & 12).
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; the School will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure the School are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of the School and DPO and all information the School are required to share about how the School use and process their personal data (via privacy notices)
  - For all personal data that the School hold, maintaining an internal record of the type of data, data subject, how and why the School are using the data, any third-party recipients, how and why the School are storing the data, retention periods and how the School are keeping the data secure

## **15. Data security and storage of records**

The School 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 students 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, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment (see School's ICT Acceptable Use Policy)
- Where the School need to share personal data with a third party, the School carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

## **16. 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 the School cannot or do not need to rectify or update it.

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

## **17. Personal data breaches**

The School will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the School will follow the procedure set out in appendix 1.

When appropriate, the School will report the data breach to the ICO within 72 hours. Such breaches in a School context may include, but are not limited to:

- A non-anonymised dataset being published on the School website which shows the exam results of students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a School laptop containing non-encrypted personal data about students

## **18. Training**

All staff and governors are provided with data protection awareness/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.

## **19. Links with other policies**

This data protection policy is linked to:

- Freedom of information publication scheme
- ICT Acceptable Use Policy
- Safeguarding Policy

## Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the Principal
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored In the School's GDPR Software – GDPRiS.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach

A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be documented and stored on the School's GDPiS. The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

### **Actions to minimise the impact of data breaches**

The School will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The School will review the effectiveness of these actions and amend them as necessary after any data breach.

#### **Sensitive information being disclosed via email (including safeguarding records)**

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure the School receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, the School will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- Staff laptops/USB devices. USB devices are prohibited from use with School devices to mitigate the risks of data loss. Staff access School data remotely and data remains on the School system and not on the laptop itself. Where data is stored on a laptop, the device will be encrypted using BitLocker encryption so that in the event a laptop is lost or stolen, access to the data stored upon it is restricted.

## Appendix 2: Subject Access Request

[Insert date]

Audenshaw School  
Hazel Street  
Manchester  
M34 5NB

### Re: Subject access request

Dear Mrs Monks

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Student / parent / employee / governor / volunteer  Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: <i>Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:</i> <ul style="list-style-type: none"><li>• Your personnel file</li><li>• Your child's medical records</li><li>• Your child's behaviour record, held by [insert class teacher]</li><li>• Emails between 'A' and 'B' between [date]</li></ul>

Yours sincerely

Name

## Appendix 3: Initial Response to Subject Access Request

*[Insert date]*

Dear *[name]*

### **Re: Your subject access request**

I can confirm that Audenshaw School received your request on *[date]* to see the following data that we hold about you:

- *[Summarise the data requested]*

*If you expect to respond within 1 month, insert:*

We will respond to your request within 1 month, as required under the General Data Protection Regulation (GDPR).

We don't think we will need to extend the response time, which we're able to do when requests are complex. However, if it becomes clear that we do need to extend the response period by up to 2 months, we will let you know by *[date – this will be 1 month from when you received the request]*.

*If you think the request is too complex to respond within 1 month, insert:*

In most cases, we will respond to subject access requests within 1 month, as required under the General Data Protection Regulation (GDPR). However, under article 12 (3), we are able to extend this period by up to 2 months for complex requests.

We anticipate that your request will be too complex for us to fulfil within 1 month.

In particular, *[insert more details to explain why you have judged that this request is too complex]*.

We will respond to your request by *[date – which will be 3 months from the date the request was received]* at the latest.

If you disagree with this decision, you can contact the Information Commissioner's Office by calling 0303 123 1113, or going to the following webpage: <https://ico.org.uk/global/contact-us/>

Information will be sent to you as soon as possible.

Yours sincerely

*[Name]*

## Appendix 4: Subject Access Request (Parent)

*[Insert date]*

Audenshaw School  
Hazel Street  
Manchester  
M34 5NB

**Re: Your parent's request for your data**

Dear *name of child*,

*Name of parent* has asked us to provide personal data about you. As it has been deemed you are old enough by the School, it is up to you to decide whether we should give this information over to them.

They have asked to see:

*Insert details of the personal data that the parent has requested*

Please tick a box below to let us know your response:

I am happy for the school to supply the information set out above to <i>name of parent</i> .	
I am not happy for the school to supply the information set out above to <i>name of parent</i> .	

Yours sincerely

*Name*



## Appendix 5 : Reply to Subject Access Request

*[Insert date]*

Audenshaw School

Hazel Street

Manchester

M34 5NB

### Re: Subject access request

Dear

Please find enclosed the information that you requested under the General Data Protection Regulation (GDPR).

Your name	
Your relationship with the school	Please select: Student / parent / employee / governor / volunteer  Other (please specify):
Details of the information you requested/enclosed	<i>Insert details of the specific information requested, such as:</i> <ul style="list-style-type: none"><li>• Your personnel file</li><li>• Your child's medical records</li><li>• Your child's behaviour record, held by [insert class teacher]</li><li>• Emails between 'A' and 'B' between [date]</li></ul>
Date you requested the information	
Date we supplied the information	<i>This must be within one month of the above date</i>
Format we supplied the information	<i>For example, encrypted USB stick accompanying this letter</i>

If you need any further advice relating to your subject access request, you can contact:

Mrs S Monks – Data Protection Officer

Yours sincerely

*Name*

## **Appendix 6 : Privacy Notice (Parent/Carer)**

### **Privacy notice for parents/carers – use of your child's personal data**

Under data protection law, individuals have a right to be informed about how the School uses any personal data the School hold about them. The School comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where the School are processing their personal data.

This privacy notice explains how the School collect, store and use personal data about individuals applying for jobs at the school.

The School, Audenshaw School, Hazel street, Manchester. M34 5NB are the 'data controller' for the purposes of data protection law.

The data protection officer is Mrs S Monks (see 'Contact us' below).

### **The personal data the School hold**

Personal data that the School may collect, use, store and share (when appropriate) about students includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Student and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

The School may also hold data about students that has been received from other organisations, including other schools, local authorities and the Department for Education.

### **Why the School use this data**

The School use this data to:

- Support student learning
- Monitor and report on student progress
- Provide appropriate pastoral care
- Protect student welfare
- Assess the quality of the services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

### **The legal basis for using this data**

The School only collect and use student's personal data when the law allows us to. Most commonly, the School process it where:

- The School need to comply with a legal obligation
- The School need it to perform an official task in the public interest

Less commonly, the School may also process student's personal data in situations where:

- The School have obtained consent to use it in a certain way
- The School need to protect the individual's vital interests (or someone else's interests)

Where the School have obtained consent to use student's personal data, this consent can be withdrawn at any time. The School will make this clear when the School ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using student's personal data overlap, and there may be several grounds which justify the use of this data.

## **Collecting this information**

While the majority of information the School collect about students is mandatory, there is some information that can be provided voluntarily.

To collect information from a student it is made clear whether providing it is mandatory or optional. If it is mandatory, The School will explain the possible consequences of not complying.

## **How the School store this data**

Personal information about students is kept while they are attending the School. This may also be kept beyond their attendance at the school if this is necessary in order to comply with the legal obligations. The Retention Schedule sets out how long the School keep information about students and is based on guidance provided by the [Information and Records Management Society's toolkit for schools](#)

## **Data sharing**

The School do not share information about students with any third party without consent unless the law and the policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) the School may share personal information about students with:

- The local authority – to meet the legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The student's family and representatives
- Educators and examining bodies
- The regulator i.e.. Ofsted
- Suppliers and service providers – to enable them to provide the service the School have contracted them for. The School will ensure all providers are GDPR compliant
- Positive Steps, i.e. Careers advice and work experience.
- Financial organisations
- Central and local government
- The auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

## **National Pupil Database**

The School are required to provide information about students to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#) (NPD), which is owned and managed by the Department for Education and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or welfare in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department of Education's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

### **Youth support services**

Once the students reach the age of 13, the School are legally required to pass on certain information about them to Tameside Metropolitan Borough Council as it has legal responsibilities regarding the education or training of 13-19 year olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or students once aged 16 or over, can contact the data protection officer to request that the School only pass the individual's name, address and date of birth to Tameside Metropolitan Borough Council

### **Transferring data internationally**

Where the School transfer personal data to a country or territory outside the European Economic Area, the School will do so in accordance with data protection law.

### **Parents' and students' rights regarding personal data**

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

If a subject access request is requested, and if the School do hold information about the parent and their child, the School will:

- Describe the data
- Explain why the School are holding and processing it, and how long it will be kept for
- Explain where the School got it from, if not from the parent or their child
- Explain who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If a request is to be made please contact the data protection officer.

### **Other rights**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the data protection officer.

### **Complaints**

The School take any complaints about the collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the data processing, please raise this with the School in the first instance.

To make a complaint, please contact the data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## **Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the data protection officer:

- Mrs S Monks
- 0161 336 2133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)

## **Appendix 7 : Privacy Notice (Students)**

### **Privacy notice for Students**

You have a legal right to be informed about how the School uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

We, Audenshaw School, Hazel Street, Manchester M34 5NB are the 'data controller' for the purposes of data protection law.

Our data protection officer is Mrs S Monks (see 'Contact us' below).

### **The personal data we hold**

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

### **Why we use this data**

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

### **Our legal basis for using this data**

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

## Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

## How we store this data

We will keep personal information about you while you are a student at our school. We may also keep it after you have left the school, where we are required to by law.

We have a record retention schedule which sets out how long we must keep information about students which is based on guidance provided within the [Information and Records Management Society's toolkit for schools](#).

## Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about students' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Educators and examining bodies
- Our regulator (the organisation or "watchdog" that supervises us), e.g. Ofsted.
- Suppliers and service providers – so that they can provide the services we have contracted them for. We will ensure all providers are GDPR compliant
- Positive Steps, i.e. Careers advice and work experience.
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

## National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#), which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) if you have any questions about the database.

## Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to Tameside Local Education Authority as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Once you are 16, can contact our data protection officer to ask us to only pass your name, address and date of birth.

### **Transferring data internationally**

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

### **Your rights**

#### **How to access personal information we hold about you**

You can find out if we hold any personal information about you, and how we use it, by making a '**subject access request**', as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request, please contact our data protection officer.

#### **Your other rights over your data**

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

### **Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

### **Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

- Mrs S Monks
- 0161 3362133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)



## **Appendix 8 : Privacy Notice (Suppliers)**

### **Privacy notice for suppliers used by the school**

Under data protection law, individuals have a right to be informed about how the School uses any personal data that the School hold about them. The School comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where the School are processing their personal data.

This privacy notice explains how the School collect, store and use personal data about suppliers of goods and services that the school contracts with, including their individual representatives, employees and agents ("you", "your"), in line with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The School, Audenshaw School, Hazel Street, Manchester M34 5NB are the 'data controller' for the purposes of data protection law.

The data protection officer is Mrs S Monks (see 'Contact us' below).

### **The personal data the School hold**

Personal data that the School may collect, use, store and share (when appropriate) includes, but is not restricted to:

- Names, characteristics and contact details of representatives and other individuals employed by the supplier or working on their behalf who the School liaise with, and who are carrying out duties under the contract with the School
- References, CVs and details of an individual's employment history, if collected as part of a bidding, tendering or engagement process
- Bank details and other financial information where it relates to an individual, such as operating as a sole trader
- Any other personal information necessary to fulfil the terms of a contract the School have with the supplier

If the contract with the supplier requires a visit, representatives, employees or agents to visit or carry out any work at the school site, the School may also collect, use and store:

- Information relating to the visit, e.g. the individual's company or organisation name, arrival and departure time, car number plate
- Photographs for identification purposes
- CCTV images captured in school
- Information about any access arrangements that may be required

In this case, the privacy notice for visitors to the School will also apply.

The School use this data to:

- Decide whether to engage with the supplier
- Fulfil the terms of the contract with the supplier, including payment
- Keep accurate records of the suppliers that the School use
- Identify suppliers, their representatives, employees and agents while on the school site, and keep all individuals safe
- Keep students and staff safe while the supplier or their representatives, employees or agents are on the school site
- Keep accurate records of visits to the school

### **The lawful basis for using this data**

The School only collect and use personal information when the law allows us to. Most commonly, the School use it where the need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, the School may also use personal information about where:

- Consent has been given to be used it in a certain way
- The School need to protect vital interests (or someone else's interests)

Where consent has been given for data to be used, this can be withdrawn at any time. The School will make this clear when requesting consent and explain how consent can be withdrawn if required

Some of the reasons listed above for collecting and using personal information will overlap, and there may be several grounds which justify the use of a person's data.

## Collecting this information

While the majority of the information the School collect is mandatory, there is some information that can be chosen whether or not to be provided.

Whenever the School seek to collect information, it will make it clear whether this must be provided (and if so, what the possible consequences are of not complying), or if there is a choice.

## How the School store this data

Where personal information is relevant to the contract, the School keep it according to the record retention schedule and the statutory obligations.

The School also keep personal information about suppliers, representatives, employees and agents whenever they visit the school. The School may keep it beyond the visit if this is necessary in order to comply with the legal obligations.

The record retention schedule sets out how long the School keep this information and is based on the guidance provided within the [Information and Records Management Society's toolkit for schools](#).

The School have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

The School will dispose of personal data securely when the School no longer need it.

## Data sharing

The School do not share information about suppliers or their representatives, employees or agents without consent unless the law and the policies allow them to do so.

Where it is legally required, or necessary (and it complies with data protection law), the School may share **personal information with:**

- The local authority – to meet our legal obligations to share certain information with it, such as where supplier information is relevant to a safeguarding concern
- The Department for Education
- Educators and examining bodies
- The regulator i.e. Ofsted
- Other suppliers and service providers. We will ensure all providers are GDPR compliant
- Central and local government
- The auditors – to demonstrate that we have conducted appropriate due diligence during procurement processes
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

## Transferring data internationally

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

## Your rights

### How to access the personal information the School hold about individuals

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If a subject access request is made, and if the School do hold information, the School will:

- Give a description of it
- Explain why the School are holding and processing it, and how long the School will keep it for
- Explain where the School got it from, if not from the individual
- Explain who it has been, or will be, shared with
- Explain whether any automated decision-making is being applied to the data, and any consequences of this
- Supply a copy of the information in an intelligible form

There is also a right for an individual's personal information to be transmitted electronically to another organisation in certain circumstances.

If a request is to be made please contact the data protection officer.

### Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. Individuals have the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent the data being used to send direct marketing
- Object to the use of personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the data protection officer.

## Complaints

The School take any complaints about the collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the data processing, please raise this with the School in the first instance.

To make a complaint, please contact the data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the data protection officer:

- Mrs S Monks
- 0161 336 2133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)

## **Appendix 9 : Privacy Notice (Visitors)**

### **Privacy notice for visitors to the school**

Under data protection law, individuals have a right to be informed about how the School uses any personal data that the School hold about them. The School comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where the School are processing their personal data.

This privacy notice explains how the School collect, store and use personal data about suppliers of goods and services that the school contracts with, including their individual representatives, employees and agents ("you", "your"), in line with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The School, Audenshaw School, Hazel Street, Manchester M34 5NB are the 'data controller' for the purposes of data protection law.

The data protection officer is Mrs S Monks (see 'Contact us' below).

### **The personal data the School hold**

Personal data that the School may collect, use, store and share (when appropriate) includes, but is not restricted to:

- Name
- Contact details
- Information relating to the visit, e.g. company or organisation name, arrival and departure time, car number plate
- Photographs for identification purposes for the duration of the visit
- CCTV images captured in school
- Information about any access arrangements that may be needed

### **Why the School use this data**

The School use this data to:

- Identify visitors and keep them safe while on the school site
- Keep students and staff safe
- Maintain accurate records of visits to the school
- Provide appropriate access arrangements

### **The lawful basis for using this data**

The School only collect and use personal data when the law allows us to. Most commonly, the School process it where the School need to comply with the legal obligation to keep the students and staff safe while on the school premises.

Less commonly, the School may also process personal data in situations where:

- The School need it to perform an official task in the public interest
- The School have obtained consent to use it in a certain way
- The School need to protect someone's vital interests (save a person's life, or someone else's)

Where the School have obtained consent, this consent can be withdrawn at any time. The School will make this clear when to ask for consent, and explain how to withdraw it.

Some of the reasons listed above for collecting and using personal information overlap, and there may be several grounds which justify the use of data.

### **Collecting this information**

While the majority of the information the School collect is mandatory, there is some information that can be chosen whether or not to be provided.

Whenever the School seek to collect information, it will make it clear whether this must be provided (and if so, what the possible consequences are of not complying), or if there is a choice.

## How the School store this data

The School will keep personal data while the visit is taking place at the School.

The School may also keep it beyond this, if necessary, to comply with the legal obligations.

The record retention schedule sets out how long the School keep information about visitors and is taken from guidance held within the [Information and Records Management Society's toolkit for schools](#).

The School have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

The School will dispose personal data securely when this is no longer needed.

## Data sharing

The School do not share information about visitors with any third party without consent unless the law and the policies allow them to do so.

Where it is legally required, or necessary (and it complies with data protection law) the School may share personal information about visitors with:

- The local authority – to meet the legal obligations to share certain information with it, such as where the visitor information is relevant to a safeguarding concern
- The Department for Education
- Educators and examining bodies
- The regulator i.e. Ofsted
- Suppliers and service providers – to enable them to provide the service the School have contracted them for. The School will ensure all providers are GDPR compliant
- Central and local government
- The auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- The organisation/company you are representing

## Your rights

### How to access the personal information the School hold about individuals

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them.

If a subject access request is made, and if the School do hold information, it will:

- Give a description of it
- Explain why the School are holding and processing it, and how long this is to be kept for
- Explain where the School got it from, if not from the individual
- Explain who it has been, or will be, shared with
- Explain whether any automated decision-making is being applied to the data, and any consequences of this
- Supply a copy of the information in an intelligible form

There is also a right for an individual's personal information to be transmitted electronically to another organisation in certain circumstances.

If a request is to be made please contact the data protection officer.

## **Your other rights regarding your data**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent the data being used to send direct marketing
- Object to the use of personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the data protection officer.

## **Complaints**

The School take any complaints about the collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the data processing, please raise this with the School in the first instance.

To make a complaint, please contact the data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## **Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the data protection officer:

- Mrs S Monks
- 0161 336 2133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)

## **Appendix 10 : Privacy Notice (School Workforce)**

### **Privacy notice for the school workforce**

Under data protection law, individuals have a right to be informed about how the School uses any personal data that the School hold about them. The School comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where the School are processing their personal data.

This privacy notice explains how the School collect, store and use personal data about individuals the School employ, or otherwise engage, to work at the School.

The School, Audenshaw School, Hazel Street, Manchester M34 5NB are the 'data controller' for the purposes of data protection law.

The data protection officer is Mrs S Monks (see 'Contact us' below).

### **The personal data the School hold**

The School process data relating to those the School employ, or otherwise engage, to work at the School. Personal data that the School may collect, use, store and share (when appropriate) includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

The School may also collect, store and use information that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

### **Why the School use this data**

The purpose of processing this data is to help us run the school, including to:

- Enable staff to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards students
- Support effective performance management
- Inform the recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

## The lawful basis for using this data

The School only collect and use personal information when the law allows us to. Most commonly, the School use it where the School need to:

- Fulfil a contract the School have entered into
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, the School may also use personal information where:

- Consent is to be used it in a certain way
- The need to protect vital interests (or someone else's interests)

Where consent has been given for data to be used, this can be withdrawn at any time. The School will make this clear when requesting consent and explain how consent can be withdrawn if required

Some of the reasons listed above for collecting and using personal information will overlap, and there may be several grounds which justify the use of a person's data.

## Collecting this information

While the majority of the information the School collect is mandatory, there is some information that can be chosen whether or not to provide to us.

Whenever the School seek to collect information, the School make it clear whether this must be provided (and if so, what the possible consequences are of not complying), or if there is a choice.

## How the School store this data

Personal data is stored in line with the Data Protection Policy.

The School create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to the individual's employment.

Once a person's employment with us has ended, the School will retain this file and delete the information in it in accordance with the record retention schedule which is based on guidance provided within the [Information and Records Management Society's toolkit for schools](#).

## Data sharing

The School do not share information with any third party without consent given unless the law and the policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), the School may share personal information with:

- The local authority – to meet the legal obligations to share certain information with it, such as safeguarding concerns.
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- The regulator i.e. Ofsted
- Suppliers and service providers – to enable them to provide the service the School have contracted them for, such as payroll. The School will ensure all providers are GDPR compliant
- Financial organisations
- Central and local government
- The auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations



- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

### **Transferring data internationally**

Where the School transfer personal data to a country or territory outside the European Economic Area, the School will do so in accordance with data protection law.

### **Your rights**

#### **How to access the personal information the School hold about individuals**

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them.

If a subject access request is made, and if the School do hold information, the School will:

- Give a description of it
- Explain why the School are holding and processing it, and how long this will be kept for
- Explain where the School got it from, if not from the individual
- Explain who it has been, or will be, shared with
- Explain whether any automated decision-making is being applied to the data, and any consequences of this
- Supply a copy of the information in an intelligible form

There is also a right for an individual's personal information to be transmitted electronically to another organisation in certain circumstances.

If a request is to be made please contact the data protection officer.

#### **Your other rights regarding your data**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. Individuals have the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent the data being used to send direct marketing
- Object to the use of personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the data protection officer.

### **Complaints**

The School take any complaints about the collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the data processing, please raise this with the School in the first instance.

To make a complaint, please contact the data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

### **Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the data protection officer:

- Mrs S Monks
- 0161 336 2133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)

## **Appendix 11 : Privacy Notice (Governors and Volunteers)**

### **Privacy notice for Governors and other volunteers.**

Under data protection law, individuals have a right to be informed about how the School uses any personal data the School hold about them. The School comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where the School are processing their personal data.

This privacy notice explains how the School collect, store and use personal data about individuals working with the school in a voluntary capacity, including Governors.

The School, Audenshaw School, Hazel Street, Manchester. M34 5NB, are the 'data controller' for the purposes of data protection law.

The data protection officer is Mrs S Monks (see 'Contact us' below).

### **The personal data the School hold**

The School process data relating to those volunteering. Personal data that the School may collect, use, store and share (when appropriate) includes, but is not restricted to:

- Contact details
- References
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

The School may also collect, store and use information that falls into "special categories" of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

### **Why the School use this data**

The purpose of processing this data is to support the school to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing Governors' details
- Facilitate safe recruitment, as part of the safeguarding obligations towards students
- Undertake equalities monitoring
- Ensure that appropriate access arrangements can be provided for volunteers who require them

### **Use of your personal information for marketing purposes**

Where consent is given to do so, Audenshaw School may send you marketing information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you. Consent can be withdrawn or the choice of 'opting out' of receiving these texts and/or emails at any time by contacting the data protection officer.

### **The lawful basis for using this data**

The School only collect and use personal information when the law allows us to. Most commonly, the School use it where it is needed to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, the School may also use personal information about where:

- Consent has been given to be used in a certain way
- The School need to protect vital interests (or someone else's interests)

Where consent has been given for data to be used, this can be withdrawn at any time. The School will make this clear when requesting consent and explain how consent can be withdrawn if required

Some of the reasons listed above for collecting and using personal information will overlap, and there may be several grounds which justify the use of a person's data.

## **Collecting this information**

While the majority of the information the School collect is mandatory, there is some information that can be chosen whether or not to be provided.

Whenever the School seek to collect information, it will make it clear whether this must be provided (and if so, what the possible consequences are of not complying), or if there is a choice.

## **How the School store this data**

Personal data is stored in accordance with the Data Protection Policy.

The School maintain a file to store personal information about all volunteers. The information contained in this file is kept secure and is only used for purposes directly relevant to work with the School.

When the relationship with the School has ended, it will retain and dispose of the personal information in accordance with guidance set out in the [Information and Records Management Society's toolkit for schools](#).

Guidance on the retention of governor records begins on page 37.

## **Data sharing**

The School do not share information with any third party without consent unless the law and the policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) the School may share personal information with:

- Government departments or agencies – to meet the legal obligations to share information about governors/trustees
- The local authority – to meet the legal obligations to share certain information with it, such as details of governors
- Suppliers and service providers – to enable them to provide the service the School have contracted them for, such as governor support. The School will ensure all providers are GDPR compliant
- Professional advisers and consultants
- Employment and recruitment agencies
- Police forces, courts

## **Transferring data internationally**

Where the School transfer personal data to a country or territory outside the European Economic Area, they will do so in accordance with data protection law.

## **Your rights**

### **How to access the personal information the School hold about individuals**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If a subject access request is made, and if the School do hold information, it will:

- Give a description of it
- Explain why the School are holding and processing it, and how long it will be kept for
- Explain where the School got it from, if not from the individual
- Explain who it has been, or will be, shared with
- Explain whether any automated decision-making is being applied to the data, and any consequences of this
- Supply a copy of the information in an intelligible form

There is also a right for an individual's personal information to be transmitted electronically to another organisation in certain circumstances.

If a request is to be made please contact the data protection officer.

### **Your other rights regarding your data**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. The right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent the data being used to send direct marketing
- Object to the use of personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the data protection officer.

### **Complaints**

The School take any complaints about the collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the data processing, please raise this with the School in the first instance.

To make a complaint, please contact the data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

### **Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the data protection officer:

- Mrs S Monks
- 0161 336 2133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)

## **Appendix 12 : Privacy Notice (Job Applicants)**

### **Privacy notice for job applicants**

Under data protection law, individuals have a right to be informed about how the School uses any personal data the School hold about them. The School comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where the School are processing their personal data.

This privacy notice explains how the School collect, store and use personal data about individuals applying for jobs at the school.

The School, Audenshaw School, Hazel street, Manchester. M34 5NB are the 'data controller' for the purposes of data protection law.

The data protection officer is Mrs S Monks (see 'Contact us' below).

Successful candidates should refer to the privacy notice for the school workforce for information about how their personal data is collected, stored and used, this will be issued as part of the induction pack.

### **The personal data the School hold**

The School process data relating to those applying to work at the school. Personal data that the School may collect, use, store and share (when appropriate) includes, but is not restricted to:

- Contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships

The School may also collect, store and use information that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

### **Why the School use this data**

The purpose of processing this data is to aid the recruitment process by:

- Enabling us to establish relevant experience and qualifications
- Facilitating safe recruitment, as part of the safeguarding obligations towards students.
- Enabling equalities monitoring
- Ensuring that appropriate access arrangements can be provided for candidates that require them

### **The lawful basis for using this data**

The School only collect and use personal information when the law allows us to. Most commonly, the School use it where the need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, the School may also use personal information where:

- Consent is given to be used in a certain way
- The School need to protect vital interests (or someone else's interests)

Where consent has been given for data to be used, this can be withdrawn at any time. The School will make this clear when requesting consent and explain how consent can be withdrawn if required

Some of the reasons listed above for collecting and using personal information will overlap, and there may be several grounds which justify the use of a person's data.

### **Collecting this information**

While the majority of the information the School collect is mandatory, there is some information that can be chosen whether or not to provide to us.

Whenever the School seek to collect information, it will make it clear whether this must be provided (and if so what the possible consequences are of not complying), or if there is a choice.

## **How the School store this data**

Personal data the School collect as part of the job application process is stored in line with the Data Protection Policy.

When it is no longer required, the School will delete the information in accordance with the [\*Information and Records Management Society's toolkit for schools\*](#) (see page 42).

## **Data sharing**

The School do not share information with any third party without consent unless the law and the policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) the School may share personal information with:

- Suppliers and service providers – to enable them to provide the service the School have contracted them for, such as HR and recruitment support. The School will ensure all providers are GDPR compliant.
- Professional advisers and consultants
- Employment and recruitment agencies

## **Transferring data internationally**

Where the School transfer personal data to a country or territory outside the European Economic Area, the School will do so in accordance with data protection law.

## **Your rights**

### **How to access the personal information the School hold about individuals**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If a subject access request is made, and if the School do hold information, the School will:

- Give a description of it
- Explain why the School are holding and processing it, and how long this will be kept for
- Explain where the School got it from, if not from the individual
- Explain who it has been, or will be, shared with
- Explain whether any automated decision-making is being applied to the data, and any consequences of this
- Supply a copy of the information in an intelligible form

There is also a right for an individual's personal information to be transmitted electronically to another organisation in certain circumstances.

If a request is to be made please contact our data protection officer.

### **Your other rights regarding your data**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent the data being used to send direct marketing
- Object to the use of personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing

- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the data protection officer.

## Complaints

The School take any complaints about the collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the data processing, please raise this with the School in the first instance.

To make a complaint, please contact the data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the data protection officer:

- Mrs S Monks
- 0161 336 2133
- [monkss@audenshawschool.org.uk](mailto:monkss@audenshawschool.org.uk)