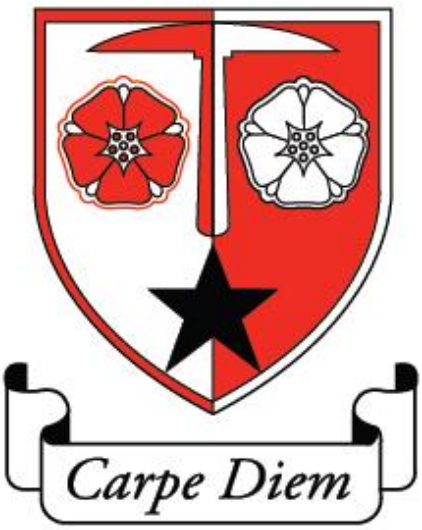
Audenshaw School



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
2.3	Sarah Monks	29/08/2024	07/10/204	07/10/2024	Full review

CONTENTS

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 UK General Data Protection Regulation (UK-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 UK-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
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The School is the Data Controller for the personal information that we process about students, parents, staff, visitors, governors and others. This means that we are responsible for the data and make decisions on how it is processed.

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. The Governing Board will also make sure that adequate resources are available to implement this policy effectively.

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 United Kingdom (UK)
    - 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 UK-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/carer 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.

7.1.1. Consent

In situations where the school has sought consent to process personal data, individuals can withdraw their consent or change their preferences at any time by contacting the school office.

7.1.2. Consent and Children

Personal data about a child (individual under 18) belongs to them and not their parent or legal guardian. However some of our students are too young or may have vulnerabilities that impact their ability to make their own decisions regarding their personal data. In such cases, consent will be sought from the parent or legal guardian.

As a rule of thumb, it is typically accepted in educational settings that students aged 13 and over are mature enough to understand their data protection rights; the school will seek consent from the parent or legal guardian for children under this age. The school will however assess this rule on a case-by-case basis to account for older children that may have vulnerabilities.

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 have a statutory obligation to share personal data relating to our students and workforce with the Local Authority and Department for Education (DfE). The sharing of data underpins school funding and educational attainment policy and monitoring in the UK.

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/carer 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 United Kingdom, the School will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

All individuals have rights with regards to their own personal data, or that of their child in respect of parents of children under the age of 13. The School will implement adequate provisions to ensure it can fulfil these rights effectively.

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 13 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 in most cases
- 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 childStaff must raise any concerns they have about disclosing personal data to the DPO who will assess whether or not exemptions apply to withhold the data from the requester.

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 where that processing is optional
- 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 UK
- 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. 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.

11. 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

12. Photographs and videos (images)

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 or legal guardians upon admission for images of students to be taken for communication, marketing and promotional materials. Once students reach the age of 13, they will be provided with the opportunity to update their preferences regarding the use of their images; in practical terms, this will likely occur at the beginning of Year 9.

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.

13. 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

14. 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). A minimalist approach to data sharing will be adopted to ensure it is limited to what is strictly necessary.

15. 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.

The school has implemented a 'Records Management Policy and Retention Schedule' that provides guidance on how long records should be kept.

16. 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

17. 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.

18. Links with other policies

This data protection policy is linked to:

- Freedom of information publication scheme
- ICT Acceptable Use Policy
- Safeguarding Policy
- Records Management Policy and Retention Schedule

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 Data Breach Log.
- 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 Data Breach Log. The DPO and Principal with 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: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behaviour record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

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 *name of parent*.	
I am not happy for the school to supply the information set out above to *name of parent*.	

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 UK-General Data Protection Regulation (UK-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	*Insert details of the specific information requested, such as:* • *Your personnel file* • *Your child's medical records* • *Your child's behaviour record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*
Date you requested the information	
Date we supplied the information	*This must be within one month of the above date*
Format we supplied the information	*For example, encrypted USB stick accompanying this letter*

If you would like to find out more about how and why the school process personal data, please visit our website to review our latest privacy notices.

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

Mrs S Monks – Data Protection Officer

Yours sincerely

Name

Privacy Notice – Parents

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Audenshaw School must process the personal data of its Students and parents to fulfil our statutory and operational duties as an education provider.

As part of our obligations under the UK General Data Protection Regulation (UK-GDPR) we must inform you what personal data we process about you, why we need it and how it is used and managed. This information is provided in the following privacy notice.

Data Controller

The school is the 'Data Controller' for the personal information that we process about you. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

The categories of Student information that we process:

The school process the following categories of information about Students and their families; this information forms the key Student record evidencing their educational development:

Students:

- Student name, address and contact details.
- Unique Student Number (UPN)
- Characteristics including gender, first language, ethnicity and religion.
- Allergies and special dietary requirements.
- Special educational needs (SEN) and medical records.
- Safeguarding and behaviour records.
- Attendance and absence records.
- Assessment and progress records.
- After-school club and extra-curricular activities records.
- School meal records (free and paid)

Parents:

- Name, address and contact details.
- Emergency contact information.
- Proof of identity and parental responsibility (where required)
- NI number (free school meal entitlement).
- Payment records (meals, trips, uniforms etc)

Alongside the Student record, the following information about Students will be processed throughout their time at school:

- Images – CCTV

- images – Identification
- Images – Promotional activities such as displays to celebrate achievements *
- Images – Biometric fingerprint (lunchtime system and access to services) *
- Usage – Logs of activity on school software, apps and digital systems.
- Usage – Internet activity.
- Consent – Records of when consent has or has not been provided.

** Information will only be processed with permission.*

Why we collect and use Student information.

We collect and use Student information, for the following purposes:

a) to support Student learning
b) to safeguard Students
c) to monitor and report on Student attainment progress.
d) to provide appropriate pastoral care
e) to assess the quality of our services
f) to keep Students and members of the school community safe
g) to meet the statutory and legal duties placed upon us
h) to meet our operational duties as an organisation
i) to correspond with Students and their families
j) to promote the school and provide an insight into school life.

The lawful basis for processing personal data

Under the UK-GDPR, we must have a lawful basis to process personal data; personal data is any data that can identify a living individual. The school rely on the following lawful bases when we process personal data relating to Students and their families:

1. The school must process personal data to meet a **legal obligation** namely;

Category	Law	Purpose for Processing
Admissions	School Admissions Code (2014)	Administer admissions & appeals process.
Education	Childrens Act (1989)	Submission of data for research
	Education Act (1996)	Submission of census data to Local Authority & DfE.
	Education Act (2005) Education & Inspections Act (2006) Education & Skills Act (2008) Childcare Act (2006)	School improvement & accountability (Ofsted)
	Education Regulations (2002)	Effective management of school
	Education (Information about Individual Students, England) Regulations 2013)	School funding and attainment monitoring
Equalities	Equality Act (2010)	Protect individuals by preventing discrimination.

Health & Safety	Health & Safety at Word Act (1974)	Providing a safe & secure environment
Safeguarding	Safeguarding Act (2006)	Safeguarding of Children
	Keeping Children Safe in Education (2024)	
	Working Together to Safeguard Children (2018)	
SEND	Children & Families Act (2014) – Special Educational Needs & Disability Code of Practice (2014)	Provide support & pastoral care

***Please contact the school office if further information is required about our legal obligations.**

2. Personal data is processed in the performance of a **public task** for example:

    - The use of CCTV to create a secure environment and to aid in crime prevention and detection.
    - Data is processed in the act of providing a full-time education to Students; our curriculum.

3. The school has a **contractual obligation** to process personal data for instance when taking payment from parents for school meals and trips.

4. The school has a **legitimate interest** to process personal data when providing educational resources and services to Students. Such activities are not part of the statutory curriculum but complement the Student's education, examples include access to classroom resources and learning apps.

5. **Consent** has been provided for the school to process data; consent is reserved for situations when the use of data is optional such as including Students in promotional images and using Student fingerprints to access the lunchtime system and other school services.

6. The school must process personal data in the act of protecting or saving someone's life; there is a **vital interest**. This lawful basis will typically apply in situations where we must share details with emergency services and first aiders if an incident or accident has occurred.

Special category data

Special category data is information that we process that is much more sensitive in nature such as details about health and wellbeing and characteristics including gender, ethnicity and religion. The school must take extra measures to ensure such information is secure and confidential, therefore we must meet an additional lawful basis from the UK-GDPR.

When processing special categories of personal data in the routine running of the school, we rely upon the following conditions:

1. **Explicit consent** (written) has been provided to make a referral to an outside agency for support with their childs health and wellbeing; this will typically involve the sharing of Student records containing special category data.

2. Personal data is processed for reasons of **substantial public interest** including:

    - Sharing special categories of personal data about Students with the government to meet our legal and statutory obligations; submitting census data to the DfE for instance.
    - Collecting special categories of personal data for equal opportunities monitoring to ensure all of our Students receive equal treatment.

- Referring serious safeguarding concerns about a Student's health and wellbeing to the police and social services; situations where parental consent is not appropriate.

3. The school must process special category data in the act of protecting or saving someone's life; there is a **vital interest**. We have a duty to inform emergency services of any known allergies, medical conditions and religious preferences if an accident occurs.

In certain circumstances, the school may be required to process personal data (including special category) for the following reasons:

- If the school is involved in a legal claim that involves you or your child; in such instances, we are processing personal data as part of or in defence of **legal claims and other judicial acts**.

- The school may be instructed to partake in public vaccination programs and health monitoring in situations where there is a threat to health such as a pandemic. In such instances, our lawful basis to process Student health records is for **reasons of public interest in the area of public health.**

Consent & Children

Consent will be sought directly from you as the parent or carer for any data processing that is optional. Although a Students personal data belongs to them, due to their age they are not typically deemed mature enough to understand their rights with regards to their personal data.

Where consent is the lawful basis relied upon for the processing of personal data, you have the right to withdraw your consent or change your preferences at any time by contacting the school office.

Collecting Student information

Most of the personal data that we collect about Students is provided directly by you as the parent or carer upon admission to the school. Records for each Student will also be transferred to us from the previous school where applicable; data is transferred securely through the electronic school to school system.

As Students progress through their educational journey with us, information is collated by the school and our staff; we will also receive information from third party agencies if Students require additional support such as therapists reports and health care plans.

In certain circumstances, the police and local authority may provide us with information they have received about a Student and / or their family that raises a safeguarding concern. Such information will be logged and monitored on the Students safeguarding record.

Student data is essential for the school's operational use. Whilst the majority of Student information provided to us is mandatory, some of it requested on a voluntary basis. In order to comply with data protection legislation, we will inform you at the point of collection, whether you are required to provide certain Student information to us or if you have a choice in this.

Storing and retaining Student data

To comply with the UK-GDPR, the school only keep personal data for as long as necessary to meet our legal and operational duties.

Our 'Records Management Policy & Retention Schedule' (available at our school office) outlines how long Student records are kept and how we determine and manage these periods. As a rule of thumb, Student educational records are kept until the childs 18th birthday, whilst safeguarding and health related records are kept until the Student reaches 31.

Personal data about Students and their families is stored securely on site. Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

School staff and those third parties accessing key Student records are subject to DBS checks and strict confidentiality agreements.

Who we share Student information with and why?

The school do not share information about Students without consent unless the law and our policies allow us to do so.

The school routinely share Student information with the following third parties to fulfil our legal duties:

- Schools that the Student attends once leaving us.
- The Local Authority
- The Department for Education
- Youth Support Services
- NHS

Appendix A provides further details on statutory data sharing.

In addition to statutory data sharing, Student data is shared with the following third-party providers of services to fulfil our operational duties as an education provider:

- ICT to give Students access to the necessary school systems.
- Information Management Software Providers to help us manage Student information more effectively.
- Classroom Apps & Software to provide Students with access to learning resources.
- Caterers to manage lunchtime provision more effectively.

In certain circumstances, we also share Student data with the following organisations:

- Auditors to ensure we are complaint and meet best practice standards.
- Third party support agencies if assistance is required to support a Student's health and wellbeing or educational development (therapists, psychologists etc).
- Police and emergency services if an accident or incident has occurred.
- Professional advisors if assistance is required to support the school with legal advice.
- Governing bodies if an incident or accident has occurred and we have a duty to report the details to them. Examples include the HSE and ICO.
- Insurance provider if we must enact a claim to which you are a party.
- Courts if we are party to a legal claim that involves you and your child.

Checks are performed on third parties with whom we share personal data to ensure they meet the high levels of data protection compliance and security expected by the school. The school take a minimalist approach to data sharing and only provide the limited amount of data if it is strictly necessary.

Transferring data internationally

We do not routinely transfer the personal data of Students and their families outside of the United Kingdom (UK). However, some of our software providers will store data remotely on servers outside of the UK, typically within the European Economic Area (EEA) whose member states must also comply to the same high standards set out in the UK-GDPR.

The school will not share any personal data with such providers or any third parties outside of the UK unless we are satisfied that they meet the necessary conditions of the UK-GDPR for international data processing.

Requesting access to your personal data and your rights

Under data protection legislation you have the right to request access to the personal data that the school holds about you and your child. You have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete.
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- to restrict our processing of your personal data (i.e., permitting its storage but no further processing).
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics.
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

Under data protection law, individuals also 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.
- object to the use of your personal data for 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 make a request, please contact your respective school office in the first instance.

The school office along with the Data Protection Officer (DPO) will support you with your request; a response will be provided within one calendar month. The school has a legal right to extend this period by a further two months for any requests deemed complex, we will however inform you of our intentions to extend the response time within one calendar month.

Complaints

If you have any concerns at all about how we process your personal data, please contact us in the first instance so that we can help resolve any issues.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

Information Commissioners Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.

Appendix 1: Why we must share Student data?

Data shared between educational settings.

When a Student transitions between educational settings, their educational record moves with them; this is a legal obligation placed on each school to allow each setting to adequately provide an education and support to Students. Any transfers completed between educational settings are carried out using secure file transfer systems including the DfE's school to school system (S2S) and the Child Protection Online Monitoring and Safeguarding system (CPOMs). Checks are made to confirm the Students next destination prior to any transfer taking place.

Youth Support Services

Once Students reach the age of 13, the School are legally required to pass on certain information about them to the Local Authority. The Local Authority have a statutory obligation to provide youth support services, post-16 education and training and careers services to Students age 13-19.

Once Students reach the age of 16 or over, a request can be made to limit the data shared with the Local Authority to the name, address and date of birth.

The NHS & School Nurse

From time to time, the school is part of immunisation programmes and other statutory and routine medical programmes that require us to share Student data with the NHS. Please note that we do not administer any immunisations or healthcare without the explicit consent of parents or carers.

Local Authority & Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our Students with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under section 3 of The Education (Information About Individual Students) (England) Regulations 2013.

The National Student Database (NPD) is owned and managed by the DfE and contains information about Students in Schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including Schools, local authorities and awarding bodies.

We are required by law, to provide information about our Students to the DfE as part of statutory data collections; the school census is an example of when we share data. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-Student-database-user-guide-and-supporting-information.

We may be required to share information about our Students with the local authority to ensure that they can conduct their statutory duties under

- the Schools Admission Code, including conducting Fair Access Panels.

Privacy Notice – Students

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Under data protection law, the school must inform you about how and why we use your personal data (information about you). We do this by providing privacy notices that explain what data we collect, why we need it and how it is used. You can also find information about the rights you have regarding your personal data.

Data Controller

The school is the Data Controller for your personal information. This means that we are responsible for it and make decisions about how it used.

We have appointed a Data Protection Officer (DPO) who helps to ensure that the school complies with data protection law. The DPO is also on hand to answer any questions or concerns you have about our use of your data. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

The personal data we process

The following information forms the basis of your educational record and is processed throughout your time at school. We get some of this information from your parent or guardian when you join our school and some is also sent to us from your previous school. The remainder is collated by us:

- Student name, address, contact details and unique pupil reference number (UPN)
- Characteristics including gender, first language, ethnicity and religion.
- Allergies and special dietary requirements.
- Special educational needs (SEN) and medical records.
- Safeguarding and behaviour records.
- Attendance and absence records.
- Assessment and progress records.
- School meal records (free and paid)

Along with your educational record, the school will also collect and process the following information that helps us to provide you and other students with a safe and engaging learning environment:

- Images – CCTV
- images – Identification
- Images – Promotional activities such as displays to celebrate achievements *
- Images – Biometric fingerprint (lunchtime system and access to services) *
- Usage – Logs of activity on school software, apps and digital systems.
- Usage – Internet activity.
- Consent – Records of when consent has or has not been provided.

** Information will only be processed with permission from you or your parent or guardian.*

Monitoring

The school has a system that monitors student use of the internet and other digital systems to make sure you are safe online and only access what you need to complete your school work. Any inappropriate use will be automatically reported to the online safety representative at school.

Why we need your personal data?

The school need your personal data to provide you with an education and to help ensure that you have the very best prospects for the future. We also process your information to keep you safe whilst in our care and provide support to protect your health and wellbeing and that of others within the school community.

Our lawful basis to process your data

Under data protection law, the school must meet a lawful basis to process your data; a lawful basis is a condition that helps to make sure we have good reason to use your information. For the most part we process your data to comply with the law. For example, the Department for Education (DfE) require us to collect data about you to help them monitor and improve education and support for young people across the UK.

We also process data in the public interest which means that your data helps to ensure that you and others in the school community are kept safe and protected and have equal opportunities.

Consent

Whilst most of the data we process about you is mandatory, sometimes the use of your information is optional. For example when we include you in images for our social media pages or ask for the use of your fingerprint to access the lunchtime system and other services. Depending on your age, we will ask for consent from either you or your parent or guardian to use your data in this way. As a rule of thumb, it is accepted that you can provide your own consent once you reach 13years old.

When the use of your data is optional, you (or your parent or guardian) can withdraw consent or change your preferences at any time by contacting the school office.

Please visit the school office if you are unhappy about our use of your images or other data.

Special Category Data

Under data protection law, information about you that is more sensitive in nature is referred to as special category data. Examples include information about your health and wellbeing and special characteristics like your gender and ethnicity.

When processing this type of data, we will typically seek consent unless there is a legal reason to do so in which case we rely upon the lawful basis of 'substantial public interest'. For example, if we think you are at risk of harm, we will share your data with the local authority and police who will help to keep you safe; we do not need consent to do this.

The DPO is available if you would like to find out more about the lawful bases we use.

Where your data is held?

Information that we hold about you is held securely on the school site in both paper and digital format. We also use software programs to store and manage your data; sometimes these programs are cloud-based and store your data in locations external to the school but usually within the UK.

Any software that holds your data must meet our high standards of security. If hosted outside of the UK, we will make sure that the provider is compliant with data protection law.

How long is your data kept?

The school will only keep your information for as long as we have a purpose to keep it; we will securely dispose of any day to day information that we no longer need once you leave school. More important information like your educational record is kept at least until you reach the age of 25.

Who we share your data with?

We only tend to share your data if the law asks us to do so, or if it helps us to provide better support and services to you and other students.

The law asks that we share your information with the following parties:

- Schools or colleges that you attend after leaving us to help you transition easily
- The local authority need your data to provide support to you and the school
- The Department for Education (DfE) who analyse student data to improve education standards across the UK
- Youth support services (if you are age 13+) to provide you with careers advice
- NHS if there are immunisations and medical programs available at school

We will also share your data with other organisations that help us to run the school effectively and provide you with a better education and experience at school. Examples include:

- The IT company that provide you with access to the school email and computer system
- The lunchtime system that allows you to easily pick and pay for your school meals

- Classroom apps and software to help with your development

In certain circumstances we may need to share your data with organisations like the police, emergency services, local authority and government if:

- We are worried about your safety and ask for help to protect you
- You have been involved in an accident or incident and we need to get help or report the details to comply with the law

The school will always make sure that if we share your data it is done so securely and only includes what it necessary.

Your data protection rights

Data protection law allows you (or your parent depending on your age) to ask us:

- For access to the information that we hold about you
- To change your information if you think it is wrong or out of date
- To delete your information if there is no valid purpose to keep it
- To restrict the use of your data and ask for a review if you are unhappy with why or how we are processing it
- To object to certain ways that we use your data
- Not to apply automated decision making to your data if it is likely to have a significant impact on your wellbeing

We ask that any requests are made by your parent or guardian if you are under the age of 13. We will accept requests from you if you are over the age of 13 but may seek the opinion of your parent or guardian if we feel it is necessary to do so. If we receive a request from your parent or guardian, we will ask for your permission for them to act on your behalf where necessary; this will typically only apply if you are over the age of 13.

We respond to most requests within one month and in most cases will not charge you a fee. If your request is complex we may extend this by a further two months (3months in total) but we will tell you in the first month if we plan to extend your request.

Complaints

If you are unhappy or concerned about how and why we use your data, please let us know so that we can help to resolve your worries. You can visit the school office or contact the DPO.

You can also complain to the Information Commissioners Office (ICO) who govern data protection in the UK if you feel the school has not resolved your concerns: https://ico.org.uk/make-a-complaint/data-protection-complaints/data-protection-complaints/

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.

Privacy Notice – Contractors

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Audenshaw School must collect and process personal data when we appoint a company as a contractor and provider of services to the school. Personal data will likely relate to key contacts of the company that the school liaise with and staff of the company that are contracted to carry out work.

This privacy notice outlines what personal data we collect, why we need it and how it is used. The school process all personal data in accordance with the UK General Data Protection Regulation (UK-GDPR) and Data Protection Act (2018).

Important Information: Any contractors and / or their staff that visit the school site should review our visitor privacy notice; information outlined in this document covers our contractual relationship with the company only.

Data Controller

The school is the 'Data Controller' for the personal information that we process in relation to contractors. This means that we are responsible for the data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

The personal data that we process

Depending upon the type of agreement the school has with the contractor, some of all of the following categories of personal data will be processed:

- Names and contact details of key personnel that will liaise with and work with the school as part of the initial set up of the agreement and those conducting any work thereafter.
- Proof of key personnels appropriateness to conduct the work associated with the agreement. This includes but is not limited to:
    - CV
    - References
    - Proof of experience and qualifications
    - Accreditations (safe contractor etc)
    - Insurance
    - DBS and vetting checks
- Bank details to fulfil payments as per the agreement with the contractor; financial data will only be classed as personal data under the UK-GDPR if the contractor is a sole trader (data is identifiable to one person).
- Any other personal information necessary to fulfil the terms of a contract the school have with the supplier; work logs, correspondence, reports etc

In the event that an incident occurs involving contractor personnel, the school will process details of the incident and associated records. Particularly if the incident breaches school policy or the terms of the agreement between the school and contractor.

Why we need this data?

The school use this data to:

- Decide whether to engage with the contractor
- Fulfil the terms of our contract with the contractor
- Ensure a fair procurement process
- Meet the requirements of any tenders or bidding programs the school participates in
- Keep accurate records of the contractors the school use
- Ensure contractor personnel are adequate to perform the tasks associated with the agreement
- Keep the school, its buildings and assets and members of the school community safe

Lawful bases for processing the data

Under the UK-GDPR, the school must have a lawful basis to process personal data. In respect of contractors we will process personal data to meet a **contractual obligation**, namely data is processed to:

- Take steps to enter into a contract with your company
- Fulfil the terms of a contract that we have with your company

In addition, we must process personal data to meet a **legal obligation**. In relation to contractors this will typically include compliance with health and safety and safeguarding laws in respect of assessing the appropriateness of contractor personnel to perform their duties safely and in line with the law and school policies.

Special Category Data

The school does not routinely process 'special category data' about contractor personnel . Special category data is information that is much more sensitive in nature and therefore requires extra protection. Examples include details about an individual's health and wellbeing and special characteristics like gender, religion and ethnicity.

It is only anticipated that the school would process special categories of personal data about contractor personnel if:

- An accident or incident occurs involving contractor personnel whilst performing their duties
- The contractor informs the school of any health and wellbeing conditions about their personnel that the school need to be aware of

When processing special categories of personal data, the school is required to meet a further lawful basis from the UK-GDPR. It is expected that data would be processed:

- For reasons of **employment, social security and social protection** (recording and reporting accidents and providing reasonable adjustments for individuals with medical conditions)
- To protect the **vital interests** of the individual or a third party; protecting or saving the life of someone.

In the event that an accident or incident results in litigation involving; the school rely upon the following conditions to process contractor special categories of data:

- **Legal claims and judicial acts:** we must process special category personal data to fulfil court proceedings, obtain legal advice or establish or defend our legal rights in any way.
- **Substantial public interest (insurance):** we need to share details of an accident or incident with our insurers.

Who we share your personal information with?

The school will only share personal data if it is necessary to fulfil a legal or operational obligation. In certain circumstances, the school may be required to share contractor personal data with the following parties:

- Local Authority: if an incident has occurred and the school requires support
- The Department for Education: if relevant to the contractors role
- Ofsted and other auditors / regulators to assess compliance and best practice
- Regulators such as HSE and ICO if we need to report an incident
- Police and other emergency services if there is an incident
- Professional advisors if the school require legal assistance following an incident
- Insurance providers if the school is subject to a claim the contractor is party to
- Courts if the school and contractor are party to litigation
- Providers of software that the school use to store contractor data (financial management system, Microsoft etc)

The school perform strict checks on those third parties with whom we share data to ensure they are complaint with data protection law and meet the same high standards of security as expected by the school.

If we must share data, we take a minimalist approach to ensure only the necessary amount of information is provided. Data will not be transferred unless there is a secure method of exchange.

Freedom of Information

As a public authority, the school may be required from time to time to share information about contractors and the services that we procure to the public if a request is received under the Freedom of Information Act (FOIA). This helps to ensure the schools procurement process is transparent.

The FOIA provides exemptions to ensure that no personal data will be publicised as part of this process unless the school deem it reasonable to do so. Similarly, the school will not disclose any information that we deem to impact the commercial interests of the school and / or contractor.

Do we transfer your data internationally?

The school do not routinely transfer data outside of the United Kingdom. In the event that we must do so, we will ensure that any exchange of data is done so compliantly and with appropriate safeguards in place.

How we store and how long we keep your personal information?

To comply with the UK-GDPR, the school only keep personal data for as long as necessary to meet our legal and operational duties.

Our 'Records Management Policy & Retention Schedule' (available at our school office) outlines how long records are kept and how we determine and manage these periods. As a rule of thumb, contractor data will be kept for up to 6years.

Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Any physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

School staff and those third parties accessing key pupil records are subject to DBS checks and strict confidentiality agreements.

What are your rights – Subject Access Requests

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 (Data Controller) in certain circumstances.

Other data protection rights

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 (DPO). The school will provide a response to a request within one calendar month; a fee will not typically be charged. The school reserves the

right to extend a request by a further two calendar months if we deem it to be complex, we will inform the individual within the first month with any intention to extend.

The school reserve the right to verify the identity of requesters where necessary.

Complaints

The school ask that any concerns regarding our use of personal data are raised with us in the first instance to help us resolve any issues. Complaints should be made directly to the DPO. Individuals can also complain to the Information Commissioners Office (ICO) if they are unhappy with how we are processing their personal data:

Information Commissioners Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.

Privacy Notice – Visitors

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Audenshaw School must collect and process personal information (data) about you when you visit our site in order to effectively manage your visit and to meet the legal obligations placed upon us as an organisation and education provider.

This privacy notice outlines what data we collect about you when you visit our site, why we need it and how it is used. The school process all personal data in accordance with the UK General Data Protection Regulation (UK-GDPR) and Data Protection Act (2018)

Data Controller

The school is the 'Data Controller' for the personal information that we process about you. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

What personal data do we process about you, where we get it and why we need it?

All visitors to the school site must provide us with the following information upon arrival to help us meet our safeguarding and health & safety obligations.

All Visitors

All visitors to site will directly input the following information into the electronic visitor screen at reception:

- Full name to identify who you are.
- Contact details to correspond with you.
- The reason for your visit to verify the legitimacy of your attendance.
- Entry and exit times to meet our health and safety obligations if there is a fire or other emergency.
- Vehicle registration to effectively manage our parking provision and ensure only permitted cars are on site.

Once the above information is inputted, an image of you will be taken and printed onto an ID badge that you must wear for security and safeguarding purposes.

Depending upon the nature of your visit, we will ask you to provide us with the following information:

- A DBS certificate to meet our safeguarding requirements and ensure we comply with the statutory duties placed upon us as a school. We log your reference number and date of check only; we do not keep a copy of your DBS certificate.

CCTV

Closed Circuit Television (CCTV) is in place at the school site; the system will capture images of you when you visit us. CCTV helps us to ensure site security and supports in the prevention and detection of crime.

Incidents & Accidents

If an incident or accident occurs on site that you are party to, we will record the details to meet our health & safety and safeguarding obligations. Examples include completing accident forms and reporting more significant incidents to the emergency services and relevant governing bodies.

Lawful Bases and Purposes for Processing

Under the UK-GDPR, the school must have a lawful basis to process your personal data. Your data is primarily processed as the school has a **legal obligation** that requires us to process it, namely:

Single Central Record

The Department for Education (DfE) statutory guidance on safeguarding 'Keeping Children Safe in Education' states that all schools must produce and maintain a record of vetting checks for certain visitors and contractors attending and working on site. Details of visitors where necessary will be logged on the schools 'single central record' (SCR). The school must log basic identifiers such as name, contact details and reason for visit along with the dates and reference numbers of the relevant vetting checks.

Health & Safety

The school has a duty to keep a log of who is on site to keep you and other members of the school community safe under health and safety law and the fire safety regulations we must adhere to; if there is a fire or accident on site, we need to be aware of your presence on site.

Legal Claims

In the event that the school is subject to a legal claim to which you are a party to, we may need to process your personal data in the enactment or defence of that claim. For instance, if an accident or incident has taken place involving you.

Further lawful bases…

We use CCTV to enhance site security, keep members of the school community safe and to aid in the prevention and detection of crime. We are **performing a task in the interest of the public**.

In the unlikely event of an accident or incident on site that involves you, we may need to process your personal data in the act of protecting or saving your life or that of another person. For instance, if we provide your name and contact details to the emergency services. In such scenarios, we have a **vital interest** to process your personal data.

Special Category Data

The school does not routinely process 'special category data' about you when you visit our site. Special category data is information that is much more sensitive in nature and therefore requires extra protection. Examples include details about your health and wellbeing and special characteristics like gender, religion and ethnicity.

It is only anticipated that the school will process special categories of personal data about you if the following scenarios occur:

- An accident or incident occurs whilst you are on site, and we must fill out an accident form or process your data in the act of providing you with assistance.

- You inform us of any specific medical conditions or requirements that we need to be aware of to ensure we can accommodate your visit accordingly.

In such cases we are processing your personal data under the following lawful basis in respect of your special category data:

- **Substantial public interest:** we are processing your special category data to support you and meet our statutory obligations under the Health & Safety at Work Act (1974) and Equalities Act (2010).

Less commonly, we may need to rely upon the following lawful basis to process your special category personal data if the school is subject or party to a legal claim involving you:

- **Legal claims and judicial acts:** we must process your special category personal data to fulfil court proceedings, obtain legal advice or establish or defend our legal rights in any way.
- **Substantial public interest (insurance):** we need to share details of an accident or injury with our insurers.

Who we share your personal information with?

The school will only share your personal data if it is required to meet a legal obligation or an operational duty relating to visitor management.

The school routinely share visitor data with the provider of our electronic visitor management system which you will input your data directly into upon arrival at our reception.

We may share your personal data with external auditors who ensure good record keeping compliance. Auditors will typically attend site and your data will not be transferred out of the school.

If there is a significant accident or incident that you are party to whilst on school site, we may share your personal information with the following:

- Local Authority
- Police
- Emergency Services
- Governing Bodies (HSE, ICO etc)
- Professional Advisors
- Insurance Provider
- Courts

The school perform strict checks on those third parties with whom we share your data to ensure they are complaint with data protection legislation and meet the same high standards of security as expected by the school.

If we must share data, we take a minimalist approach to ensure only the necessary amount of information is provided. Data will not be transferred unless there is a secure method of exchange.

Do we transfer your data internationally?

The school do not routinely transfer visitor data outside of the United Kingdom, however some of the third parties with whom we share your personal data may store data on international servers. In such circumstances, we will ensure the relevant safeguards are in place and data protection standards are complied with fully.

How we store and how long we keep your personal information?

To comply with the UK-GDPR, the school only keep personal data for as long as necessary to meet our legal and operational duties.

Our 'Records Management Policy & Retention Schedule' (available at our school office) outlines how long visitor records are kept and how we determine and manage these periods. As a rule of thumb, general visitor data will be kept for up to 12months.

Your personal data is stored securely on site. Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Any physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

School staff and those third parties accessing key pupil records are subject to DBS checks and strict confidentiality agreements.

What are your rights?

Under the UK-GDPR, you have a right to access the personal data that we hold about you by making a subject access request (SAR). If you make a SAR and we do process the data you have requested access to, we will:

- Give you a description of it.
- Explain why we are processing it and how long we will hold it.
- Explain where we collected the data if not from you.
- Outline if the data has been or will be shared with any other parties.
- Inform you if any automated decision making has been applied to the data and provide any consequences of this.
- Provide you with a copy of the data in an intelligible form.

Along with the right to access your personal data, you also have the following rights under the UK-GDPR:

- The right to ask us to rectify any personal information you feel is inaccurate or incomplete.
- The right to ask us to erase your personal data in certain circumstances.
- The right to ask us to restrict the processing of your personal data in certain circumstances.
- The right to object to the processing of your personal data in certain circumstances
- The right to ask us to transfer the personal data you provided to another organisation in certain circumstances.

If you would like to exercise any of your rights, please contact the school office in the first instance.

A response will be provided to you within one calendar month. The school reserves the right to extend the response time by a further two calendar months if your request is complex, we will however inform you of any intention to extend within the first month.

Complaints

If you have any concerns at all about how we process your personal data, please contact us in the first instance so that we can help resolve any issues.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

Information Commissioners Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.

Privacy Notice – Workforce

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Audenshaw School must process the personal data of our employees to ensure that we can meet the terms of your employment contract and fulfil our legal and administrative obligations as an employer.

As part of our obligations under data protection law, namely the UK General Data Protection Regulation (UK-GDPR) we must inform you how and why we process your personal data. The following privacy notice outlines what data we process about you as an employee, why we need it and how it is used.

This privacy notice applies to all employees of the school including those working with us on a temporary and voluntary basis. For the purposes of this privacy notice, we will refer to all parties as 'employees' of the school.

Data Controller

The school is the 'Data Controller' for the personal information that we process about you. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

The personal data that we process about you and why we need it:

The school will process the following categories of personal data about you before and during your employment with us:

Recruitment & Induction:

We process the following data about you to assess your suitability for the role, correspond with you during your employment and meet the legal and statutory duties placed upon us by the Department for Education who require us to submit data about our staff as part of the workforce census:

- Personal identifiers: Name, address and key contact details.
- Next of kin and emergency contact details.
- Special characteristics: D.O.B, gender, religion, place of birth and ethnicity.
- Employment and education history.
- Qualifications necessary to your role.
- Personal statement.

The school must partake in staff safer recruitment checks to meet our safeguarding obligations. Some or all of the following checks will be conducted on you and logged on your record:

- Identification (photo and address)
- DBS (renewed every three years)
- References
- Qualified Teacher Status
- Prohibition of Teachers & Management
- Non-British National Status
- Social Media Checks

We will also conduct and record a 'Right to Work' checks where applicable if your country of origin is not the UK. Similarly, occupational health checks will be performed should you disclose any health & wellbeing

concerns to us that may impact your ability to perform your role. Occupational health records will be added to your personnel file.

Contractual Information

The following information is processed to fulfil the terms of your employment contract with us and to administer the payment of your salary and benefits:

- Employment contract and job description.
- Bank details
- NI number
- Payroll records: salary, hours worked, deductions (trade union subscriptions), overtime, expenses etc.
- Tax codes and submission records.
- Absences and leave records including flexible working, maternity and paternity leave.
- Pension and benefit records.

Please note that in the case of pensions and subscriptions, the school collates a limited amount of information to set up and administer the services. The respective provider store and manage your contributions and services.

Performance Information

The school process the following information to monitor your performance, support your personal development and manage any performance related issues and concerns about you:

- Reviews and appraisals including records on promotion and contractual changes.
- Training and continual professional development records.
- Disciplinary and grievance records that you are party or subject to.
- Whistleblowing concerns that you are party or subject to.

Health & Wellbeing Information

Employment and health & safety legislation requires the school to provide adequate levels of support to your health and wellbeing. As part of our compliance, we will process the following data where applicable:

- Occupational health and wellbeing records, reports and reasonable adjustments.
- Health management questionnaires.
- Fit notes and medical records received from your GP or other health agencies.
- Referrals for health and wellbeing support.
- Accident forms and records.
- Risk assessments, pregnancy and disability etc.

General Information

The following information will be processed to help the school fulfil its operational duties and to meet its security and safeguarding obligations:

- Attendance on site and external trips.
- Access to school systems including monitoring of your usage of digital systems, email and internet etc.
- Images: CCTV
- Images: promotional for the school website etc (with your consent)
- Images: ID badge and for general identification.

How we get your information

Most of the personal information we process is provided directly by you when you join the school as an employee. We will also receive information about you from third parties including:

- Previous employer in respect of references
- Providers of security checks and employee support services
- Government departments including HMRC, DfE and local authorities.
- HR and payroll providers who collate contractual and salary-based records.

Any further information will be collated by the school throughout our working relationship with you.

Most of the information provided to us about you is mandatory, we will however inform you in instances where the processing of your personal data is optional and seek your permission where necessary.

The lawful basis for processing personal data

Under the UK-GDPR, we must have a lawful basis to process personal data; personal data is any data that can identify a living individual. The school rely on the following lawful bases when we process personal data relating to you:

1. We must process your personal data to meet a **legal obligation**, namely;

Category	Law	Purpose for Processing
Recruitment	Keeping Children Safe in Education (2024) UK Visa and Immigration Law	Employment checks for the purposes of safeguarding & security.
Health & Wellbeing	Health & Safety at Work Act (1974)	Maintain a safe workplace for staff and other members of the school community.
Employment	Employment Law UK (general)	Fulfil our duties as an employer.
Data Collection & Censuses for Schools	Department for Education Statutory Data Collections	Workforce census.
Equalities	Equality Act (2010)	Protect against discrimination & provide equal opportunities.
Local Authority Data Sharing	Education (supply information about the school workforce) (England) Regulations (2007)	Statutory data sharing to local authority.

2. We must process your personal data to meet a **contractual obligation**; to fulfil the terms of your employment contract with us. For instance, we cannot pay your salary and make tax submissions without processing your name, NI number, bank details and tax codes.

3. Personal data is processed in the performance of a **public task** for example:

   - The use of CCTV to create a secure environment and to aid in crime prevention and detection.
   - Data is processed in the act of providing a full-time education to pupils.
   - Retaining an image of you for identification purposes.

4. The school has a **legitimate interest** to process your personal data; the legitimate interest could be that of the school, you as a staff member or other individuals such as our pupils. An example is using your name and school email address to provide you with access to educational programmes and software that helps to support your role and provide our pupils with learning resources.

5. The school must process personal data in the act of protecting or saving someone's life; there is a **vital interest**. This lawful basis will typically apply in situations where we must share details with emergency services and first aiders if an incident or accident has occurred.
6. You have provided your **consent** for us to process your personal data; consent will be sought for any data processing that is optional for instance when we ask you to take part in school photographs for use on our website and social media pages.

Special Category Data

Special category data is information that we process that is much more sensitive in nature such as details about your health and wellbeing and characteristics including gender, ethnicity, religion and whether or not you are a member of a trade union. The school must take extra measures to ensure such information is secure and confidential, therefore we must meet an additional lawful basis from the UK-GDPR.

When processing special categories of personal data in the routine running of the school, we rely upon the following conditions:

1. You have provided your **explicit consent (written)** to the processing for instance when we make a referral to external agency for health and wellbeing support to help with your employment, and we need to exchange information about your health with them.

2. The school must process your personal data in the field of **employment, social security and social protection**. This condition covers the processing of your special category data to meet our legal obligations as an employer and education provider. Examples include:

    - Processing your ethnicity and place of birth to fulfil right to work checks.
    - Processing your health data as part of the first aid process if you have an accident, collating data about you if occupational health checks are required and logging information about your health if you are off sick.

3. Your personal data is processed in situations where there is a **substantial public interest**. This lawful basis will typically apply in the following scenarios:

    - We must submit special characteristics such as your gender and ethnicity to the DfE as part of the workforce census for equal opportunities monitoring.
    - If you are party to or subject to a safeguarding concern and we must make a referral to the relevant third-party agencies, and it is not appropriate to seek your consent.

4. The school must process your special category data in the act of protecting or saving yours or the life of someone else; there is a **vital interest**. We have a duty to inform emergency services of any known allergies, medical conditions and religious preferences if an accident occurs.

In certain circumstances, the school may be required to process personal data (including special category) for the following reasons:

- If the school is involved in a legal claim that involves you; in such instances, we are processing personal data as part of or in defence of **legal claims and other judicial acts**.

- The school may be instructed to partake in public vaccination programs and health monitoring in situations where there is a threat to health such as a pandemic. In such instances, our lawful basis to process your health records is for **reasons of public interest in the area of public health.**

Consent

Where consent is the lawful basis for processing, you have the right to withdraw your consent or change your preferences at any time by contacting the school office.

Storing and retaining your data

To comply with the UK-GDPR, the school only keep personal data for as long as necessary to meet our legal and operational duties.

Our 'Records Management Policy & Retention Schedule' (available at our school office) outlines how long your records are kept and how we determine and manage these periods. As a rule of thumb, most of your records are held on your staff personnel file and kept for a period of 6years post-employment. Information relating to your salary and tax contributions is kept for 6years from the date of the current tax year to which they relate.

Personal data is stored securely on site. Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

If we must transfer your data to third parties, we will ensure this is done so using secure transfer methods.

School staff and those third parties accessing key records are subject to DBS checks and strict confidentiality agreements.

Sharing your personal information

The school do not share your personal data with third parties unless the law or our policies permit us to do so. The school must partake in statutory data sharing with the following third parties to meet our obligations under the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments:

- The Local Authority
- The Department for Education

You can find out more about our statutory data sharing requirements in appendix 1.

In addition to our statutory data sharing, we outsource a number of key services that are vital to the functioning of the school. As part of this process, we will share your data with the following providers where applicable:

- HR & Payroll Provider
- ICT & System Providers
- Training Providers
- Educational Software & Resource Providers (to provide you with an account and access)
- Trade Unions and Professional Associations
- Professional Advisors & Consultants (solicitors etc)
- Auditors (to ensure compliance and best practice standards are being met)

In certain circumstances, we may be required to share your data with the following parties:

- Your emergency contacts if you are involved in an accident.
- Police and emergency services if there is an accident / incident involving you.
- NHS, occupational health and other third-party health and wellbeing agencies if you require additional support and reasonable adjustments to assist with your role.
- Ofsted if your data is relevant to an inspection.
- Examining bodies if your data is relevant to a check to ensure we are meeting examination regulations.
- Governing bodies such as the HSE and ICO if there is a significant accident / incident involving you.
- Insurance provider(s) if there is a claim involving you.
- Courts if there is a legal claim that involves you.

Checks are performed on third parties with whom we share personal data to ensure they meet the high levels of data protection compliance and security expected by the school. The school take a minimalist approach to data sharing and only provide the limited amount of data if it is strictly necessary.

Transferring data internationally

We do not routinely transfer your personal data outside of the United Kingdom (UK). However, some of our software providers will store data remotely on servers outside of the UK, typically within the European Economic Area (EEA) whose member states must also comply to the same high standards set out in the UK-GDPR.

The school will not share any personal data with such providers or any third parties outside of the UK unless we are satisfied that they meet the necessary conditions of the UK-GDPR for international data processing.

Requesting access to your personal data and your rights

Under data protection legislation, you have the right to request access to the personal data that the school holds about you. You have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified if it is inaccurate or incomplete.
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- to restrict our processing of your personal data (i.e., permitting its storage but no further processing).
- to object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics.
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

Under data protection law, individuals also 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.
- object to the use of your personal data for 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 make a request, please contact the school office in the first instance.

The school office along with the Data Protection Officer (DPO) will support you with your request; a response will be provided within one calendar month. The school has a legal right to extend this period by a further two months for any requests deemed complex, we will however inform you of our intentions to extend the response time within one calendar month.

Complaints

If you have any concerns at all about how we process your personal data, please contact us in the first instance so that we can help resolve any issues.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

Information Commissioners Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.

Appendix 1: How the government uses your data

The workforce data that we lawfully share with the Department for Education (DfE) through data collections:

- informs the Department for Education (DfE) policy on pay and the monitoring of the effectiveness and diversity of the school workforce.
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department for Education (DfE)

The Department for Education (DfE) may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department for Education (DfE) has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the Department for Education (DfE) releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data, they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Privacy Notice – Governors

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Audenshaw School must collect and process personal information (data) about you when you are appointed as a governor of our school to meet our statutory and operational obligations. This privacy notice outlines what data we collect about you when you join the school, why we need it and how it is used.

The school process all personal data in accordance with the UK General Data Protection Regulation (UK-GDPR) and Data Protection Act (2018).

Data Controller

The school is the 'Data Controller' for the personal information that we process about you. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

What personal data do we process about you and why we need it?

We process the following general categories of personal data when you are inducted as a governor to ensure we can effectively correspond with you and provide you with the necessary resources to fulfil your role:

- Full name
- Address and Contact details (including emergency contacts)

To meet our safeguarding obligations and confirm your suitability for your role, the school will process the following information about you:

- Proof of ID (photo and address)
- DBS check (only reference and date of check kept)

As an education provider in the UK, the school must process the following further categories of personal data about you to meet the statutory obligations place upon us by the Department for Education.

- Postcode, D.O.B and any previous names.
- Role
- Governor ID
- Dates and Means of Appointment
- Declaration of Pecuniary and Personal Interests
- Attendance at Meetings (including minutes)

The following general information will also be processed by the school during your role with us (**where applicable**) to meet our further legal and operational duties:

- CCTV: records images for site security if you visit the school.
- Health & Safety: logs of your visits to site.
- Health & Safety: medical information or access requirements declared to us by you.
- Health & Safety: accident / injury records.
- Compliance: records of training you partake in.
- Usage Data: access and usage of school systems and records.

- Incidents: records of any concerns about you or incidents that you are party to.

Where we get your information?

Most of the personal information that we process is provided directly by you upon induction to your role. Further information will be collated by the school as your role with us progresses.

We receive a small amount of information about you from third parties, this is typically limited to the results of your DBS check and other third-party service providers; ICT access to our systems and training providers issuing your certificates etc.

Whilst most of the information that we process is mandatory, we will inform you if there are any data processing activities that are optional and seek your permission where necessary.

Our lawful basis for processing your personal data?

Under the UK-GDPR, the school must have a lawful basis to process your personal data. Your data is primarily processed as the school has a **legal obligation** that requires us to do so. All maintained schools have a legal duty to provide governance information as part of the following statutory regulations:

- Section 538 of The Education Act (1996)

As part of these statutory regulations, general information about you and your role is published by the Department for Education (DfE) on their 'Get Information about Schools' (GIAS) website:

https://get-information-schools.service.gov.uk/

We must also publicise information about you and your role on the school website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online#governors-information-and-duties

Further legislation and regulations that require us to process your personal data include:

- Health & Safety at Work Act (1974): providing a safe and secure working environment and the recording and reporting of accidents and injuries.
- Keeping Children Safe in Education (2024): compiling DBS checks for the safeguarding of children in our care and managing any concerns raised.

Further lawful bases to process your data:

When processing your personal data to provide you with access to systems and fulfilling your training requirements, the school has a **contractual obligation** to process your personal data; the school is processing your data to provide you with resources you need to fulfil the agreement between you and the school.

The school has implemented a CCTV system that will record images of you should you visit the school as part of your role. The system enhances site security and aids in the prevention and detection of crime; the school are therefore processing personal data for the performance of a **public task**.

In the event that an accident or incident occurs that involves you, we may be required to process your personal data in the act of protecting or saving your life or that of another person; we have a **vital interest** to process your personal data.

Special Category Data

The school does not routinely process special category data about you; special category data is information that is much more sensitive in nature such as details about your health and special characteristics like gender, ethnicity and religion.

Such data will typically only be processed by the school should you inform us of any health concerns that may impact your role, allergies, disabilities, access requirements etc or you are involved in an accident / incident on our site.

When processing special category data, we must meet an additional lawful basis from the UK-GDPR. The school rely upon **substantial public interest** to process special category data for the above purposes, namely, to meet the obligations the government place on us under Health & Safety Law.

Less commonly, if an accident or incident involving you is referred to a court or legal claim, we may be required to process your special category data under the lawful basis of **legal claims and judicial acts**.

Who we share your personal information with and why?

The school will only share your personal data if it is required to meet a legal obligation or an operational duty relating to your role as governor.

The school must share your personal data with the DfE to meet our duties under the aforementioned Academies Handbook; your information will also be shared with the public via the school and DfE websites to promote transparency on how the school is run. **Appendix 1** provides further information on how the DfE use your personal data.

Data publicised about you by the school is limited to what is strictly necessary, namely your basic governor profile and any reference to you in meeting minutes.

We also share your data with the following third-party providers of key services to the school:

- ICT to create and manage your school email account and access to the relevant areas of the school system.
- DBS check provider to meet our safeguarding obligations.
- Governor information management system (Trust Governor) to set up an account and provide access to the information and resources needed to perform your duties.
- Auditors to ensure that the school is compliant and meets best practice standards.

The school **may** share your data with the following parties if you are involved in or the subject of an accident or incident:

- Local Authority
- Police
- Emergency Services
- Governing Bodies (HSE, ICO etc)
- Professional Advisors
- Insurance Provider
- Courts

The school perform strict checks on those third parties with whom we share your data to ensure they are complaint with data protection legislation and meet the same high standards of security as expected by the school.

If we must share data, we take a minimalist approach to ensure only the necessary amount of information is provided. Data will not be transferred unless there is a secure method of exchange.

Do we transfer your data internationally?

The school do not routinely transfer your data outside of the United Kingdom, however some of the third parties with whom we share your personal data may store data on international servers. In such circumstances, we will ensure the relevant safeguards are in place and data protection standards are complied with fully.

How we store and how long we keep your personal information?

To comply with the UK-GDPR, the school only keep personal data for as long as necessary to meet our legal and operational duties.

Our 'Records Management Policy & Retention Schedule' (available at our school office) outlines how long records are kept and how we determine and manage these periods. As a rule of thumb, general information about you is kept for 6years once your appointed role ceases whilst key meeting minutes and documentation is kept for the life of the school.

Your personal data is stored securely on site. Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Any physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

School staff and those third parties accessing key pupil records are subject to DBS checks and strict confidentiality agreements.

What are your rights?

Under the UK-GDPR, you have a right to access the personal data that we hold about you by making a subject access request (SAR). If you make a SAR and we do process the data you have requested access to, we will:

- Give you a description of it.
- Explain why we are processing it and how long we will hold it.
- Explain where we collected the data if not from you.
- Outline if the data has been or will be shared with any other parties.

- Inform you if any automated decision making has been applied to the data and provide any consequences of this.
- Provide you with a copy of the data in an intelligible form.

Along with the right to access your personal data, you also have the following rights under the UK-GDPR:

- The right to ask us to rectify any personal information you feel is inaccurate or incomplete.
- The right to ask us to erase your personal data in certain circumstances.
- The right to ask us to restrict the processing of your personal data in certain circumstances.
- The right to object to the processing of your personal data in certain circumstances
- The right to ask us to transfer the personal data you provided to another organisation in certain circumstances.

If you would like to exercise any of your rights, please contact the school office in the first instance.

A response will be provided to you within one calendar month. The school reserves the right to extend the response time by a further two calendar months if your request is complex, we will however inform you of any intention to extend within the first month.

Complaints

If you have any concerns at all about how we process your personal data, please contact us in the first instance so that we can help resolve any issues.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

Information Commissioners Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.

Appendix 1: How the government uses your information

The governance data that we lawfully share with the Department for Education (DfE) via GIAS will:

- increase the transparency of governance arrangements.
- enable local authority-maintained schools, academies, academy trusts and the Department for Education (DfE) to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context.
- allow the Department for Education (DfE) to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role.

Data collection requirements

To find out more about the requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors

Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to authorised Department for Education (DfE) and education establishment users with a Department for Education (DfE) Sign-in (DSI) account who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the Department for Education (DfE) unless the law allows it.

How to find out what personal information the Department for Education (DfE) hold about you:

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you

- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a subject access request (SAR). Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact DfE: https://www.gov.uk/contact-dfe

Privacy Notice – Applicants

Date: Aug 2024

Review Date: Aug 2025

Version: 1

Document owner: Audenshaw School

A: Hazel Street, Audenshaw, Manchester, M34 5NB

T: 0161 336 2133 | E: admin@audenshawschool.org.uk

Introduction

Audenshaw School must process your personal data when you apply for a job role with us in order to review your application and assess your suitability for the role in question. To meet our obligations under the UK General Data Protection Regulation (UK-GDPR), we must inform you about how and why we process your personal data; this information is outlined in the following privacy notice.

Data Controller

The school is the 'Data Controller' for the personal information that we process about you during the recruitment process. This means that we are responsible for your data and make decisions on how it is used.

Data Protection Officer

The school has appointed a Data Protection Officer (DPO) who is responsible for overseeing compliance with the relevant data protection legislation. Our DPO provides support to the school and acts as the first point of contact for any questions or queries regarding data protection. Our DPO is Mrs Monks who can be contacted on:

T: 0161 336 2133 | E: monkss@audenshawschool.org.uk

What personal data do we process about you and why we need it?

Application Stage:

We collect the following personal data directly from you as part of your application to assess your suitability for the role and fulfil our employment, equality and safeguarding obligations:

- Name & contact details
- D.O.B and NI number
- Gender, ethnicity and religion
- Education history and qualifications
- Employment history
- Medical conditions or disabilities that may affect your employment.
- Details of any criminal convictions you wish to make us aware of.
- Referee details
- Personal statement

Shortlisting:

If you are shortlisted for a position, we will collate the following personal information to support with our interview and selection process:

- Interview notes & correspondence with you
- References that include details of your conduct, any grievance or performance issues, appraisals and attendance.
- Pre-employment checks

Selection:

If you application is successful and a conditional offer is made, you will be subject to a number of pre-employment checks which will be recorded as part of your recruitment record. The school will collate the following pre-employment check records where applicable:

- Photographic ID: proof of identity
- Evidence of Qualifications: certificates etc to confirm suitability.

- DBS: safeguarding and security.
- Right to Work: legal obligation to check entitlement to work in the UK.
- Occupational Health: if you have disclosed a health & wellbeing concern that may impact on your role with the school.
- Prohibition of Teachers & Management: confirm suitability for role.

Once your pre-employment checks have been completed and approved, any records relating to the recruitment process will form the basis of your personnel file. A staff privacy notice will be issued to you upon induction which outlines how staff personal data is processed.

Where we get your information?

Most of the information that we process will be provided directly from you as part of your application, we will also receive data from your previous employer(s) when requesting references. Further information such as interview notes and pre-employment checks will be collated by us as part of the recruitment process.

The information that we process about you is mandatory to meet our legal obligations and operational duties as an employer and education provider. We will however inform you in situations where data processing is optional.

The lawful basis for processing personal data

Under the UK-GDPR, we must have a lawful basis to process personal data; personal data is any data that can identify a living individual. The school rely on the following lawful bases when we process your personal data:

- We have a **contractual obligation** to process your personal data; more specifically, we are taking steps towards entering into a potential employment contract with you when you apply for a job with us.

- We have a **legal obligation** to perform pre-employment checks for safer recruitment and safeguarding under 'Keeping Children Safe in Education' (2024). We must process characteristics like your gender and ethnicity to meet our obligations under the Equalities Act (2010) to prevent discrimination. Further government regulations and employment law requires that we perform further checks such as 'Right to Work' in the UK.

<u>Special Category Data</u>

Special Category Data is information about you that is much more sensitive in nature, examples include details about your health and wellbeing and special characteristics like your religion, gender and ethnicity. The school must meet an additional lawful basis from the UK-GDPR to process such data, we rely upon the following:

- The processing of your data is necessary to meet our obligations in the field of **employment, social security and protection**. For instance, if we must check your eligibility to work in the UK or exchange health information about you with Occupational Health professionals.

- The processing is necessary for reasons of **substantial public interest**, particularly when processing special characteristics about you such as gender and ethnicity to ensure we meet our obligations as an equal opportunity's employer and performing pre-employment checks to meet our safeguarding obligations.

Less commonly, we may be required to process your personal data in the act of protecting or saving your life or that of another person in emergency situations. Our lawful basis for processing your personal data in such scenarios is to protect the **vital interests** of yourself or another third party.

Similarly, if the school is involved in a legal claim that involves you, we may need to process your data for the purposes of **legal claims and other judicial acts**.

Storing and retaining your data

To comply with the UK-GDPR, the school only keep personal data for as long as necessary to meet our legal and operational duties.

Our 'Records Management Policy & Retention Schedule' (available at our school office) outlines how long your records are kept and how we determine and manage these periods. As a rule of thumb, unsuccessful applications will be kept for 6months from the date we appoint the successful candidate. If your application is

successful, it will form part of your personnel file which will be kept for a period of 6years post-employment with the school.

Personal data is stored securely on site. Records kept in electronic format are stored securely on carefully selected databases and systems that are fully encrypted with password protection and two factor authentication utilised where available. Physical records are kept in locked cabinets within locked offices and archive rooms; key access is strictly limited depending upon role.

If we must transfer your data to third parties, we will ensure this is done so using secure transfer methods.

School staff and those third parties accessing key records are subject to DBS checks and strict confidentiality agreements.

Who we share your personal information with?

The school does not routinely share your personal data with any third parties unless your application is successful, at which point your data will be exchanged with the following third parties where applicable:

- DBS provider
- Occupational Health provider
- Government (checking eligibility to work in education).

From time to time, the school is subject to statutory and non-statutory audits. As part of this process, auditors will perform random checks on our records to ensure that we comply with best practice standards in recruitment; your personal data may be reviewed as part of such audits.

We only provide the limited amount of data necessary to fulfil each activity respectively. Any third parties with whom we share data are subject to a compliance check to ensure they meet the same high standards of data protection compliance and security as the school.

We do not process recruitment records outside of the UK unless the law or our policies require us to do so. In such circumstances, we will ensure the relevant safeguards are in place and data protection standards are complied with fully.

What are your rights?

Under the UK-GDPR, you have a right to access the personal data that we hold about you by making a subject access request (SAR). If you make a SAR and we do process the data you have requested access to, we will:

- Give you a description of it.
- Explain why we are processing it and how long we will hold it.
- Explain where we collected the data if not from you.
- Outline if the data has been or will be shared with any other parties.
- Inform you if any automated decision making has been applied to the data and provide any consequences of this.
- Provide you with a copy of the data in an intelligible form.

Along with the right to access your personal data, you also have the following rights under the UK-GDPR:

- The right to ask us to rectify any personal information you feel is inaccurate or incomplete.
- The right to ask us to erase your personal data in certain circumstances.
- The right to ask us to restrict the processing of your personal data in certain circumstances.
- The right to object to the processing of your personal data in certain circumstances
- The right to ask us to transfer the personal data you provided to another organisation in certain circumstances.

If you would like to exercise any of your rights, please contact the school office in the first instance.

A response will be provided to you within one calendar month. The school reserves the right to extend the response time by a further two calendar months if your request is complex, we will however inform you of any intention to extend within the first month.

Complaints

If you have any concerns at all about how we process your personal data, please contact us in the first instance so that we can help resolve any issues.

You can also complain to the Information Commissioners Office (ICO) if you are unhappy with how we have used your data:

Information Commissioners Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 | Website: https://www.ico.org.uk

Last Updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2024.