



Haberdashers' West Midlands Academies Trust
Data Protection and Privacy Policy
2024-2026

Haberdashers' Abraham Darby
Haberdashers' Adams

DATA PROTECTION AND PRIVACY POLICY - 2024-2026	
Named Responsibility of Policy	Mrs J Edgar – Principal Mr G Hickey – Headmaster
Date of Policy Review	February 2024
Date of next Review	February 2026
Governor Accountability	HWMAT Board of Governors
This policy will be readily accessible to Parents/Carers/Staff/Visitors/Members of the Public through the school websites	

COMMITMENT TO REVIEW

This Policy will be monitored and reviewed every two years by the relevant policy owner named and evaluated and approved by the Governing Body on a two-year cycle, and/or in the light of changes to National Curriculum requirements and DfE guidance/regulations.

Contents

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

1. Aims

Our schools aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK Data Protection Act (DPA) 2018/ UK [General Data Protection Regulation \(GDPR\)](#)

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/UK DPA 2018. It is also based on guidance published by the Information Commissioner's Office (ICO).

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	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data, which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">• 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,

	<p>recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
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

Our schools process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore are data controllers.

The schools are individually 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 our schools, Governors, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Governors

The Board of Governors has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

He/she will provide an annual report of their activities directly to the Board of Governors and, where relevant, report to the board their advice and recommendations on the schools data protection issues.

The DPO is also the first point of contact for individuals whose data the schools process, and for the ICO.

Our DPO: **Rob Montgomery, Audit & Governance Lead Manager-**
Telford & Wrekin Council
Darby House
Telford TF3 4J

T: 01952 383103

E: IG@telford.gov.uk

5.3 Headmaster or Principal

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

6. Data protection principles

The GDPR is based on data protection principles that our schools 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 fulfill 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 schools aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 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 schools 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 pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in Article 9 of the UK GDPR and UK DP 2018.

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

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

7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we 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 [Information and Records Management Society's toolkit for schools](#).

8. Sharing personal data

8.1 We may share personal data with anyone where there is a legal basis to do so and in particular when

- There is an issue with any person that puts the safety of our pupil, staff, or visitors at risk
- We need to liaise with other agencies for example trade unions – we will seek consent where necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we 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 we 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 us

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

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

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

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that their 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 preferably can submit in writing, either by letter, email to the relevant DPO, etc. They should include:

- Name of individual
- Proof of ID
- 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 relevant DPO.

9.2 Children and subject access requests

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 agreed to the request.

Above the age of 12, a child has the right to make decisions about their Personal Data, unless in the opinion of the DPO acting reasonably, a child does not display sufficient maturity to make such reasonable decisions.

If a child has not reached their 12th birthday, then a parent or legal guardian should make decisions on Personal Data, unless the child can demonstrate to the DPO that they can demonstrate exceptional maturity considered to be in advance of their age that would provide considerable assurances that they can make reasonable decisions about their Personal Data.

If two parents or legal guardians assert differing decisions regarding a child's Personal Data, then HAFT will seek clarification from the relevant authority before complying with any decisions regarding the Personal Data.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual requesting the information to complete a Subject Access Request Form (see Appendix A) in order to detail any specific information, the individual requires
- 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 unless complex
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex . We will inform the individual of this within 1 month and explain why the extension is necessary

We will not disclose information if any exemptions detailed in the UK GDPR/UK DPA 2018 apply.

If the request is unfounded or excessive, we 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, without prejudice to the generality, if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we 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 we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

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

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

10. Parental requests to see the educational record

If the school receives a written request from parents, or those with parental responsibility to access to their child's educational record (which includes most information about a pupil) it will be treated as a Subject Access Request and will be dealt with under the Pupil Information Regulations.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the [Protection of Freedoms Act 2012, UK GDPR and ICO guidance](#).

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 we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

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

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

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

12. CCTV

For the safety of our students, staff, visitors and the security of our sites, we use CCTV in various locations around both the schools sites. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the site ICT/Site Managers.

13. Photographs and videos

As part of our schools activities, we may take photographs and record images of individuals within our school. Taking and displaying images of pupils will require specific consent where the photo or video is not essential for the running of the school

We will obtain annually, written consent from parents or legal guardians or in line with recommendation from the NSPCC pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Uses of images for which this specific consent is required will include:

- Within schools on notice boards and for other day to day activities within the schools.
- Schools marketing materials, including magazines, brochures, newsletters, etc.
- Schools pictures including sports team and society pictures- which will not include names.
- Outside of schools by external agencies such as the school photographer, newspapers, campaigns.
- Online on our schools websites or social media pages- Twitter, Facebook for example.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will, where practical delete the photograph or video and not use it in future material, existing printed material will continue to be used until supplies are exhausted.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent or legal guardian and pupil.

Where we don't need parental consent-i.e., over 18 years, we will clearly explain to the pupil how the photograph and/or video will be used.

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

Photos or video taken purely for personal use are exempt from the Data Protection Act 2018, for example:

A parent takes a photograph of their child and some friends taking part in a school Sports Day or performance to be put in the family photo album. These images are for personal use and the DPA does not apply.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

14. Data protection by design and default

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

- Appointing a suitably qualified DPO, 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 data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 12 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely and in-line with our Data Retention Policy.

Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

Records will be stored in accordance with the retention guidelines specified in the Records Management Society's ['Records Management Toolkit for Schools.'](#)

For example, we will shred, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. When an external company is booked to undertake confidential shredding of waste this will always take place on site and a certificate of destruction will be obtained.

17. Personal data breaches

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

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

When appropriate, we 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 schools website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

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

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

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and shared with the full Board of Governors.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information policy
- Child Protection and Safeguarding policy
- ICT Acceptable Use policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the Headmaster or Principal and the Chair of Governors
- 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 by the DPO.
- 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 stored by the DPO.

- The DPO and Headmaster or Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We 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. We 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 we 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, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted



A member of the Haberdashers' West Midlands Academies Trust

Haberdashers' Abraham Darby

Haberdashers' Adams

Subject Access Request Form

Date submitted:

Date received:

Received by:

Haberdashers' Abraham Darby/Adams should respond to your request within one school calendar month unless it is deemed complex where up to an additional 2-month extension will be applied as allowed by the Act. However, this period does not start until:

- a) We are satisfied about your identity
- b) You have provided enough detail to locate the information you are seeking

Please complete the following sections of this form providing as much information as possible to help us deal with your request:

Step 1: Providing Information

Name of subject:
Relationship with the school e.g., Pupil / parent / employee / governor / volunteer/ If other please explain:
Address and postcode:
Contact number:
Email address:

Are you requesting information about yourself? Please circle yes or no.

Yes No

If **no**, then please provide further information:

Name of person acting on behalf of the data subject:

Relationship to the data subject:

Provide a brief explanation of why you are requesting this information rather than the subject:

Address (Including postcode) of person acting on behalf of data subject:

Email address of person acting on behalf of data subject:

Please provide written authority from the data subject including a signature or other legal documentation (e.g., power of attorney) to confirm this request.

Please provide evidence of your identity and that of the data subject (see Step 2 for details of acceptable identity)

Please provide a clear description of the information that you are requesting in the space provided to the right

Please note:

- If you provide specific details of what information you want, e.g., name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.
- Please tell us if you are looking for a specific document / piece of information – you may receive your information quicker.

This might involve:

- My personnel file
- My child's medical records
- My child's behaviour record, held by [insert class teacher]
- Emails between 'A' and 'B' between [date]

Step 2: Provide Identification

If you are the Data Subject:

- Please provide two pieces of evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.
- Driving Licence
- Passport
- National ID Card
- Medical Card
- Utility Bill

Or if you are acting on behalf of the Data Subject:

- Please provide two pieces of evidence of the identity of the Data Subject (one containing a photo)
- In addition, also provide two pieces of evidence of your identity (one including a photo)

You may wish to send your documents special/recorded delivery. Your proof of identity will be returned to you securely after verification.

All information in respect to your request will be sent to you via secure email unless alternative arrangements are made. We may require further evidence of your identity if you collect your information from the school.

Step 3: Declaration

To be completed by all applicants. Please note that any attempt to mislead Haberdashers' Abraham Darby /Adams may lead to prosecution.

I (insert name) _____,

Certify that the information given on this application form and any attachments therein to Haberdashers' Abraham Darby / Adams is accurate and true.

I understand that it is necessary for the school to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.

Signature _____

Date _____

Step 4: Return of the Form

If you are either posting your documents and payment or hand delivering them then our address is detailed below:

FAO Data Protection Officer	FAO Data Protection Officer
Haberdashers’ Abraham Darby	Haberdashers’ Adams
Ironbridge Road	High Street
Madeley	Newport
Telford	Shropshire
TF7 5HX	TF10 7BD

Section 5: How we will send you the information you have requested

We want you to receive the information you have requested in the most convenient way for you. However, we do have an obligation under the Data Protection Act 2018 to provide you with the information you have requested in the most secure way possible.

We believe the most secure way to provide you with the information is either:

- For you to collect the documentation in person from Haberdashers’ Abraham Darby via a paper or CD
- For us to email you the information securely/encrypted using our Secure Communication System which would allow you to electronically access the information requested (free of charge)

We can post your information to you but there are risks attached to providing you with your information using this method, e.g., Royal Mail may lose your information, deliver it to the wrong address, etc.

Please confirm you are happy to receive your information by our Secure Communication System by ticking the box below and confirming the email address that your information should be sent to:

Tick Box	<input type="checkbox"/>	EMAIL ADDRESSES
----------	--------------------------	-----------------

Alternatively, if you prefer any of the other methods below, please indicate which by ticking ONE of the boxes below:

Collection in person	<input type="checkbox"/>	CD or Paper Copy <i>(please circle your choice)</i>
By Post (special delivery)	<input type="checkbox"/>	CD or Paper Copy <i>(please circle your choice)</i>