

# Data Protection Policy



**Wistaston Academy**  
Primary and Nursery School  
Together We Learn • Together We Achieve

<b>Policy Author</b>	D Griffiths and S Joy
<b>Responsible Governor's Committee</b>	Business, Finance and HR
<b>Date Reviewed</b>	Autumn 2021
<b>Frequency of Review</b>	Review annually or in light of changes to legislation or operating experience

**CHANGE CONTROL**

<b>Date</b>	<b>Details of Change</b>	<b>Staff Member</b>
4.11.21	Entered time period to remove photos and videos if consent is refused or withdrawn to 12 months (12.)	SO
4.11.21	Entered time period to remove photos and videos for pupils leaving the school to 12 months (12.)	SO
4.11.21	Changed 'our 11 school's practice' to 'our schools' practice' (19.)	SO

## **Contents**

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

## 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors, suppliers, partners and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

Term	Definition
<b>Personal Data</b>	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number – e.g. UPN for pupils/employee number</li><li>• Address</li><li>• Online identifier, such as a username e.g. UPN for pupils/employee number</li><li>• Date of Birth</li><li>• National Insurance Number</li><li>• Qualifications</li><li>• Medical Information (which has been disclosed)</li><li>• Safeguarding information</li><li>• Socio Economic Data – Free School Meals assessment</li><li>• Assessment Scores</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics – where information has been disclosed</li><li>• Health – physical or mental – where information has been disclosed</li><li>• Adoption status</li></ul>

	<ul style="list-style-type: none"> <li>• Safeguarding Information</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data Subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data Controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data Processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal Data Breach</b>	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 Academy processes personal data relating to parents, pupils, staff, governors, visitors, suppliers, partners and others, and therefore is a data controller. The Academy 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 our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. This policy is for reference to parents/guardians and suppliers to demonstrate the transparency of the organisation.

**5.1 Governing board** - The Directors have overall responsibility for ensuring that our school complies with all relevant data protection obligations.

**5.2 Data Protection Officer** - The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Directors 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. Our DPO is Samantha Orme and is contactable via the Academy.

**5.3 Principal** – The Principal acts as the representative of the data controller in school on a day-to-day basis.

**5.4 All staff** - Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy

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

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 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 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 the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom applications, and we intend to rely on consent as a basis for processing, we will get parental consent.

Whenever we first collect personal data directly from individuals, we will provide them with the Trusts privacy notices.

## **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 school's records retention schedule.

## **8. Sharing Personal Data**

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as 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

We will also 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

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.

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 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

We will make transparent our information asset register which will detail the information that we hold about you and any data sharing arrangements and/or agreements that are in place and the reason for sharing this data.

Subject access requests (SAR) must be submitted in writing, either by letter, email or fax to the School c/o The DPO. On receipt of this request the school will send you a letter to confirm this has been received and ask you to complete the SAR form and provide two forms of identification. The information required to complete a SAR is:



- 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 who will advise on the response.

The Trust takes its responsibilities for Data Protection seriously and will always ask for two forms of identification to be provided.

## **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 given their consent.

Children below the age of 12 are generally not 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 pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis by the school leadership team.

## **9.3 Responding to subject access requests**

As data controllers we are obliged to check that we are conforming to the law and only sharing data where we have a legal basis to do so, therefore we will authenticate every request without exception. When responding to requests, we:

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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, 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 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
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances). This would generally be in the form of a common transfer file (CTF) via S2S which is a secure system used by schools to transfer pupil data when pupils are transferring schools.

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**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 30 school days of receipt of a written request. This is not the same request as a SAR unless the SAR is specifically asking to see educational records only.

## **11. CCTV**

We use CCTV in various locations around the school to ensure that the site remains safe. 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 and a log is kept. 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 DPO.

## **12. Photographs and videos**

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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, we will delete the photograph or video and not distribute it further within 12 months.

If a child leaves the school due to school leaver age or movement within school phase we will remove photographs and videos of the child within 12 months.

## **13. 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/experienced 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

- 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. This is known commonly as the information asset register.

#### **14. 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.

We will only release data to individuals when we have been able to authenticate that this is a legitimate request.

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
- 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 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 – please refer to the acceptable usage 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)
- Data may be accessed by staff while they are working from home/outside of the Trust school sites this must be used in accordance with their job role. The acceptable user policy must be adhered to.

## **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 we cannot or do not need to rectify or update it.

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

Further information about disposal of records is available in the data retention schedule which is available from the administration team.

## **16. Data Retention Guidelines**

The disposal of records complies with our Data Retention Schedule. This has been developed using the IRMS toolkit for schools and is available from the administration team.

## **17. Personal data breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the correct procedures. 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 school 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. 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 and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our schools' practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the Trust Board.

## **20. Links with other policies**

This data protection policy is linked to our:

- Acceptable Usage Policy
- Data Retention Schedule
- Privacy Note – Pupils
- Privacy Notice – Staff
- Safeguarding Policy
- Other School policies that refer to the usage of personal data e.g. any school policies referring to the usage of photographs and videos.