



# **POLICY DOCUMENT**

## **Data Protection Policy**

Approved by Trust  
6<sup>th</sup> November 2023

Date for review:  
November 2024

<b>Document Control</b>	
Title	Data Protection Policy
Purpose	To provide guidance and information about how the Trust will collect, store and process personal data about our pupils, workforce, parents and others.
Supersedes	Data Protection Policy <b>version 2</b>
Amendments	Added details relating to subject access requests and the rights of data subjects, added details regarding data breach procedure including ICO procedure, added information about roles and responsibilities
Related Policies/Guidance	Privacy Notice – Children, Parents/Carers. Workforce, Recruitment. Records Management Policy. Retention Schedule.
Author	John Tomlinson
Approved Level	Trust – Statutory Policy
Date adopted	6 <sup>th</sup> November 2023
Expires / Next review	November 2024
Signature of Chair	

### **Wise Owl Trust**

is a Multi Academy Trust

Registered in England and Wales number 8053288

Registered Office: Trust House, c/o Seymour Road Academy, Seymour Road South, Clayton, Manchester, M11 4PR

The Wise Owl Trust has a number of Trust-wide policies which are adopted by all the academies in the Trust to ensure an equitable and consistent delivery of provision. The Trust Board has responsibility for the operation of all academies and the outcomes of all students; however, responsibility is delegated to the Local Governing Body of each school via the Scheme of Delegation.

Within our policies reference to:

- Governing Body/Governors relate to the members of the Local Governing Body representing the Trust Board, known at Wise Owl Trust as Local School Committee Boards.
- School includes a reference to school or academy unless otherwise stated.
- Headteacher includes a reference to Headteacher, Principal or Head of School of a school or academy.

# Contents

1	Policy statement .....	4
2	About this policy.....	4
3	Definition of data protection terms .....	4
4	Roles and Responsibilities .....	4
5	Data protection principles.....	5
6	Fair and lawful processing .....	5
7	Processing for limited purposes.....	7
8	Notifying data subjects.....	7
9	Adequate, relevant and non-excessive processing .....	8
10	Accurate data.....	8
11	Timely processing .....	8
12	Processing in line with data subjects' rights.....	8
13	Data security .....	12
14	Data Protection Impact Assessments.....	14
15	Disclosure and sharing of personal information.....	14
16	Data Processors .....	14
17	Images and Videos .....	15
18	Video Surveillance.....	15
19	Data Breaches.....	15
20	Training .....	16
21	Changes to this policy.....	16
	Appendix A - Definitions .....	17
	Appendix B - Data Breach Procedure .....	19

## 1 Policy statement

- 1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities within the Wise Owl Trust, we will collect, store and **process personal data** about our pupils, workforce, parents and others. This makes us a **data controller** in relation to that **personal data**.
- 1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.
- 1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

## 2 About this policy

- 2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the retained EU law version of the General Data Protection Regulation ((EU)2016/679) ('UK **GDPR**'), the Data Protection Act 2018 and other regulations (together '**Data Protection Legislation**').
- 2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.
- 2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

## 3 Definition of data protection terms

All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in Appendix A.

## 4 Roles and Responsibilities

- 4.1 This policy applies to all staff employed by Wise Owl Trust and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.
- 4.2 The Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.
- 4.3 As a Trust, we are required to appoint a Data Protection Officer (DPO). Our DPO is Sheryl Cardwell. They are contactable via email – [s.cardwell@wiseowltrust.com](mailto:s.cardwell@wiseowltrust.com)
- 4.4 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.
- 4.5 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

## 5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

5.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

5.1.3 Adequate, relevant and not excessive for the purpose;

5.1.4 Accurate and up to date;

5.1.5 Not kept for any longer than is necessary for the purpose; and

5.1.6 **Processed** securely using appropriate technical and organisational measures.

5.2 **Personal Data** must also:

5.2.1 be **processed** in line with **data subjects'** rights;

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing of personal data** by the Trust.

## 6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing of personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**;

6.2.2 why the **personal data** is being **processed**;

6.2.3 what the lawful basis is for that **processing** (see below);

6.2.4 whether the **personal data** will be shared, and if so with whom;

6.2.5 the period for which the **personal data** will be held;

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:



- 6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
  - 6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
  - 6.4.3 where the **processing** ensures the vital interest of the individual e.g. to protect someone's life
  - 6.4.4 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
  - 6.4.5 where the **processing** is required for the legitimate interests of the Trust or a third party, provided the individual's rights and freedoms are not overridden
  - 6.4.6 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.
- 6.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:
- 6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
  - 6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
  - 6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
  - 6.5.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.
- 6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.
- 6.7 If any **data user** is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

## Vital Interests

- 6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

## Consent

- 6.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

- 6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.
- 6.11 When pupils and or our workforce join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.
- 6.12 In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.
- 6.13 If consent is required for any other **processing of personal data** of any **data subject**, then the form of this consent must:
- 6.13.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;
  - 6.13.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
  - 6.13.3 Inform the **data subject** of how they can withdraw their consent. Consent can be withdrawn at any point – please see our privacy notice.
- 6.14 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.
- 6.15 The DPO must always be consulted in relation to any consent form before consent is obtained.
- 6.16 A record must always be kept of any consent, including how it was obtained and when.

## 7 Processing for limited purposes

- 7.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).
- 7.2 We will only process **personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

## 8 Notifying data subjects

- 8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:
- 8.1.1 our identity and contact details as **Data Controller** and those of the DPO;
  - 8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;
  - 8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
  - 8.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;

- 8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;
  - 8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
  - 8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
- 8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

## 9 Adequate, relevant and non-excessive processing

We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

## 10 Accurate data

- 10.1 We will ensure that **personal data** we hold is accurate and kept up to date.
- 10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.
- 10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

## 11 Timely processing

- 11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.
- 11.2 We shall seek to comply with the rights exercised by **data subjects** as set out in section 12 below as soon as possible and within legal time limits. However, there may be instances where due to circumstances outside of the Trust's control this may not be possible e.g. where the School or Trust has been closed or is only partially operable. In such circumstances data subjects will be notified and provided details about the reason for the delay and when a response can reasonably be expected.

## 12 Processing in line with data subjects' rights

- 12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:
  - 12.1.1 request access to any **personal data** we hold about them;
  - 12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;
  - 12.1.3 have inaccurate or incomplete **personal data** about them rectified;
  - 12.1.4 restrict **processing** of their **personal data**;

- 12.1.5 have **personal data** we hold about them erased
- 12.1.6 have their **personal data** transferred; and
- 12.1.7 object to the making of decisions about them by automated means.

## The Right of Access to Personal Data

- 12.2 **Data subjects** may request access to all **personal data** we hold about them. The mechanism to do this is a **subject access request**. This applies to all data subjects we hold data on, including pupils, parents, and staff. Any requests should be directed to our DPO.
- 12.3 Requests can be made in writing or verbally; however, we ask requests are made in writing for our internal records. We ask you include:
  - the name of the data subject (if you are requesting on behalf of another, please include your relationship to the data subject)
  - details of information being requested e.g. pupil file, SEND records, records of meetings, disciplinary records
  - contact information, and preferred way of receiving the information
- 12.4 Staff are given training to recognise subject access requests, and must forward any to the DPO immediately.
- 12.5 When responding to requests, we:
  - May ask for proof of identity by requesting photographic ID
  - May ask for clarification on the information requested
  - Will respond without delay and within 1 month of receipt of request
  - Will provide the information free of charge
  - May extend the timeline by up to 3 months, where a request is complex or numerous. If this is the case, you will be informed of this within 1 month of your request and you will be informed of why the extension is necessary
- 12.6 In some cases, we may not disclose information where the legislation prevents us from doing some. Some examples are as follows:
  - If the information may cause serious harm to the physical or mental health of the subject or another individual
  - If the information may reveal that a child is at risk of abuse, where the disclosure of that information would not be in the child's best interest
  - If the information is contained in adoption or parental order records
  - If the information is given to a court in proceedings concerning the child

- 12.7 In some cases, we may refuse a request where it is deemed to be manifestly unfounded or excessive. Where we refuse a request, we will inform you why and inform you of the right to complain to the ICO.
- 12.8 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. This will be considered on a case-by-case basis. In the event that a child is not deemed mature enough to exercise their rights, a parent or guardian may also exercise this right on their behalf.
- 12.9 If the information requested by a parent in a SAR relates to the 'educational record' of a pupil in accordance with 'The Education (Pupil Information) (England) Regulations 2005', we do not have to comply with this as this only applies to local authority schools and special schools. Independent schools, academies and free schools are not obliged to respond to a request for access to a pupil's education record under this legislation. However, we will treat the request as a subject access request, and follow the procedure for handling SARs.

[GDPR Privacy Notice - Pupils](#)

[GDPR Privacy Notice - Parents/Carers, Volunteers, Students and other Visitors](#)

[GDPR Privacy Notice - Workforce](#)

[GDPR Privacy Notice - Recruitment](#)

## The Right to Object

- 12.10 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.
- 12.11 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.
- 12.12 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.
- 12.13 In respect of direct marketing any objection to **processing** must be complied with.
- 12.14 The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

## The Right to Rectification

- 12.15 If a **data subject** informs the Trust that **personal data** held about them by the Trust is inaccurate or incomplete, then we will consider that request and provide a response within one month.
- 12.16 If we consider the issue to be too complex to resolve within that period, then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.
- 12.17 We may determine that any changes proposed by the **data subject** should not be made. If this is the case, then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information

Commissioner's Office at the time that we inform them of our decision in relation to their request.

## The Right to Restrict Processing

- 12.18 **Data subjects** have a right to “block” or suppress the **processing** of personal data. This means that the Trust can continue to hold the **personal data** but not do anything else with it.
- 12.19 The Trust must restrict the **processing** of **personal data**:
- 12.19.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);
  - 12.19.2 Where the Trust is in the process of considering an objection to processing by a **data subject**;
  - 12.19.3 Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and
  - 12.19.4 Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.
- 12.20 If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.
- 12.21 The DPO must be consulted in relation to requests under this right.

## The Right to Be Forgotten

- 12.22 **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:
- 12.22.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
  - 12.22.2 When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;
  - 12.22.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
  - 12.22.4 Where the **processing** of the **personal data** is otherwise unlawful;
  - 12.22.5 When it is necessary to erase the personal data to comply with a legal obligation.
- 12.23 The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:
- 12.23.1 To exercise the right of freedom of expression or information;

- 12.23.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
  - 12.23.3 For public health purposes in the public interest;
  - 12.23.4 For archiving purposes in the public interest, research or statistical purposes; or
  - 12.23.5 In relation to a legal claim.
- 12.24 If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.
- 12.25 The DPO must be consulted in relation to requests under this right.

## Right to Data Portability

- 12.26 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.
- 12.27 if such a request is made then the DPO must be consulted.

## 13 Data security

- 13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.
- 13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
- 13.3 Security procedures include:

**Entry controls.** Any stranger seen in entry-controlled areas should be reported to the schools Designated Safeguarding Lead (DSL) or deputy Designated Safeguarding Lead.

**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 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 (see our Acceptable Use of ICT 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

**Methods of disposal.** 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 or incinerate 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.

**Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

### **Working away from the school premises – paper documents.**

Staff are advised to lock any papers or equipment away when not in use.

Only work on personal data in areas where others cannot access the information or listen into confidential calls

In line with our assessment and marking policy, there is no expectation for staff to take home books for marking purposes. Should staff take books home, the guidelines set out above must be adhered to.

### **Working away from the school premises – electronic working.**

Document printing - Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

Staff work through the most up to date version of our remote access drive.

Our cloud storage is not set to public or accessible without a username or password (or other type of authentication). Staff are forbidden from storing, transferring and transporting electronic information on Universal Serial Bus (USB) devices.

Only key staff have been given full access to the storage area. All other staff have been given read, write, edit or delete permissions where appropriate.

We are not using any default root or administrative accounts for any day-to-day activities, and they are appropriately secured.

All Work From Home (WFH) devices have the 8-digit security password function

We have checked if multi factor authentication is available and configured where possible

Wise Owl Trust Filtering and Monitoring extends to school-owned equipment in the home. This also extends to the staff Google accounts, not just the device

We have either blocked the ability to add forwarding rules to external email addresses or have a method in place to detect forwarding rules.

We have advised staff to use Wise Owl Trust email and not rely on their own email or messaging accounts for the storage or transmission of personal data.

- 13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

## 14 Data Protection Impact Assessments

- 14.1 The Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

- 14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

- 14.3 The Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

- 14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

## 15 Disclosure and sharing of personal information

- 15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency “ESFA”, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

- 15.2 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

- 15.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

- 15.4 Further detail is provided in our Schedule of Processing Activities.

## 16 Data Processors

- 16.1 We contract with various organisations who provide services to the Trust, including:

- Payroll Provider – Administration of staff pay, pensions and NI contributions
- School Meals Provider – Pupil names and details of allergies, medical conditions etc.
- Arbor – Staff and pupil data
- Parent Pay – Parent and pupil data
- Greater Manchester Pension Providers
- National College training

- 16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

- 16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.
- 16.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

## 17 Images and Videos

- 17.1 The Trust does not prohibit this as a matter of policy. For each individual event, signed consent is requested for pupils to have their photographs taken. Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. However, **it is explicitly explained to parents that any recordings or images must not be shared on any social media platforms.**
- 17.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.
- 17.3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.
- 17.4 As a Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.
- 17.5 Whenever a pupil begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

## 18 Video Surveillance

The Trust operates a CCTV system. Please refer to the Trust CCTV Policy / Video Surveillance Policy.

We use CCTV in various locations around the premises of the Trust to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask for individual permission to use CCTV, but we will clearly display CCTV warnings to inform individuals they are being recorded.

Any queries about the CCTV system can be directed towards the DPO.

## 19 Data Breaches

- 19.1 The Trust will make all reasonable endeavours to ensure there are no personal data breaches

19.2 In the event of a suspected data breach, we will follow the procedure set out in appendix 1, which is based on ICO guidance.

19.3 When appropriate, we will report the breach to the ICO within 72 hours. Such breaches may include but are not limited to:

- A non-anonymised data set being published on the Trust website
- Safeguarding information being made available to an unauthorised person
- The theft of a Trust laptop containing non-encrypted personal data

## 20 Training

Data protection will form part of continuing professional development, and staff will be provided with refresher training on a regular basis to ensure the legislation is being adhered to.

## 21 Changes to this policy

We may change this policy at any time; at minimum, the policy will be updated annually. Updated policies will be made available to data subjects.

## Appendix A - Definitions

Term	Definition
Biometric Data	is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting
Biometric Recognition System	<p>is a system that operates automatically (electronically) and :</p> <ul style="list-style-type: none"> <li>• Obtains or records information about a person's physical or behavioural characteristics or features; and</li> <li>• Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system</li> </ul>
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our workforce (including Governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making

	available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or Biometric Data
Workforce	Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees / Members, local governors, parent helpers

## Appendix B - Data Breach Procedure

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

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third-party data processors must notify the Data Protection Officer immediately.

Step 2: The DPO must notify the headteacher immediately when notified of a breach.

Step 3: The DPO will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from school staff members and any third-party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the DPO will assess the potential consequences of the breach. The DPO should consider;

- How could it affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The DPO must decide whether or not the breach must be reported to the ICO. Breaches must be considered on a case-by-case basis; however, a breach must be reported to the ICO if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation
- damage to reputation
- or any other significant economic or social disadvantage to the individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the ICO.

Step 6: The DPO will document the decision taken as to whether or not the ICO are notified of the breach. The school should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the ICO. The school should keep a record of breaches whether or not they are reported to the ICO. This record should include:

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach

- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 8: In cases where the breach must be reported to the ICO, the DPO (or another member of staff if they are not available) must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant [page on the ICO's website](#).

Step 9: The DPO must decide whether or not the individual's affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any affects and the likelihood of them being affected must guide this decision-making process. If there is a high risk the DPO will notify, in writing, all potentially affected individuals. This notification will include:

- Contact details for the DPO
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 10: The DPO must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the school or the ICO.