

# Data Protection Policy

Veritas Multi Academy Trust



|                            |                    |                        |
|----------------------------|--------------------|------------------------|
| <b>Approved by:</b>        | Trust Board        | <b>Date:</b> July 2026 |
| <b>Author:</b>             | Stephanie Sheppard |                        |
| <b>Scrutinised by:</b>     | Adam Atkinson      |                        |
| <b>Next review due by:</b> | June 2027          |                        |

## Contents

|                                                                  |    |
|------------------------------------------------------------------|----|
| 1. Aims .....                                                    | 3  |
| 2. Legislation and guidance .....                                | 3  |
| 3. Definitions .....                                             | 4  |
| 4. The data controller .....                                     | 5  |
| 5. Roles and responsibilities .....                              | 5  |
| 6. Data protection principles .....                              | 6  |
| 7. Collecting personal data .....                                | 6  |
| 8. Sharing personal data .....                                   | 7  |
| 9. Subject access requests and other rights of individuals ..... | 8  |
| 10. Parental requests to see the educational record .....        | 10 |
| 11. Biometric recognition systems .....                          | 10 |
| 12. CCTV .....                                                   | 10 |
| 13. Photographs and videos .....                                 | 11 |
| 14. Artificial intelligence (AI) .....                           | 11 |
| 15. Data protection by design and default .....                  | 12 |
| 16. Data security and storage of records .....                   | 12 |
| 17. Disposal of records .....                                    | 13 |
| 18. Personal data breaches .....                                 | 13 |
| 19. Training .....                                               | 13 |
| 20. Monitoring arrangements .....                                | 13 |
| 21. Links with other policies .....                              | 13 |
| Appendix 1: Personal data breach procedure .....                 | 14 |

---

## 1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, governors, volunteers and any other third parties.

The Trust is registered with the Information Commissioners Office (ICO) as required: ZB126347.

## 2. Legislation and guidance

This policy meets the requirements of the:

- > UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- > [Data Protection Act 2018 \(DPA 2018\)](#)
- > [Data \(Use and Access\) Act 2025](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

It also reflects the ICO's [guidance](#) 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, living individual, whether identified directly or indirectly.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> <li>o Name (including initials)</li> <li>o Identification number</li> <li>o Location data</li> <li>o Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity or personal data held visually in photographs, video clips (including CCTV) or sound recordings.</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>o Racial or ethnic origin</li> <li>o Political opinions</li> <li>o Religious or philosophical beliefs</li> <li>o Trade union membership</li> <li>o Genetics</li> <li>o Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>o Health – physical or mental</li> <li>o Sex life or sexual orientation</li> </ul>                                                                                |
| <b>Processing</b>                          | <p>Any activity that involves the use of 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, and also includes transmitting or transferring personal data to third parties.</p>                                                                                                                                                                                                                                                                               |
| <b>Data subject</b>                        | <p>The identified or identifiable individual whose personal data is held or processed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| TERM                                            | DEFINITION                                                                                                                                                                                                                                                            |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data controller</b>                          | A person or organisation that determines the purposes and the means of processing personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.                                                                 |
| <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. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing. |
| <b>Data Protection Impact Assessment (DPIA)</b> | DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.                                                                                                                                                                   |
| <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 Trust collects and processes a large amount of personal data each year. The school collects data relating to parents and carers, pupils, staff, visitors and others. The Trust collects personal data relating to staff, pupils, trustees, members, visitors and others. The Trust and each of the schools is a data controller as personal data is collected at both school and Trust level.

The Trust is registered with the ICO as 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.

### 5.1 Trustees

Trustees have overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

### 5.2 Data Protection Officer (DPO)

The Data Protection Officer is responsible for overseeing data protection within the School/Trust. Should you have any questions, concerns or queries please contact them on the following information: -

Data Protection Officer: Judicium Consulting Limited  
Address: 5<sup>th</sup> Floor, 98 Theobalds Road, London, WC1X 8WB  
Email: [dataservices@judicium.com](mailto:dataservices@judicium.com)  
Web: [www.judiciumeducation.co.uk](http://www.judiciumeducation.co.uk)  
Telephone: 0345 548 7000 (Option 1, then 1)

Please contact the DPO with any questions about the operation of this data protection policy or the UK GDPR, or if you have any concerns that this data protection policy is not being or has not been followed.

School based DPOs are as follows:

Mundella – Marie Neshet

Warden House – Adam Atkinson

Pilgrims' Way – Emma Campbell.

If contacting each of the School DPOs, please also copy in [governance.professional@veritasmat.co.uk](mailto:governance.professional@veritasmat.co.uk).

### 5.3 Headteacher

The Headteacher of each school acts as the representative of the data controller on a day-to-day basis. The Headteacher is responsible for ensuring sufficient staff training is in place and all staff are aware of their responsibilities of the policy and procedures.

### 5.4 All staff

Staff are responsible for:

- o Collecting, storing and processing any personal data in accordance with this policy, protecting the individual's right to privacy.
- o Informing the school of any changes to their personal data, such as a change of address
- o Contacting the school 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 UK
  - 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 UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- o Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- o Collected for specified, explicit and legitimate purposes (purpose limitation);
- o Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation);
- o Accurate and, where necessary, kept up to date (accuracy);
- o Kept for no longer than is necessary for the purposes for which it is processed (storage limitation);
- o Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality);
- o Not transferred to another country without appropriate safeguards in place (transfer limitation); and
- o Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

This policy sets out how the Trust 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 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- o The data needs to be processed so that the School/Trust can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- o The data needs to be processed so that the School/Trust can **comply with a legal obligation**
- o The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- o The data needs to be processed so that the School/Trust, as a public authority, can **perform a task in the public interest or exercise its official authority**
- o The data needs to be processed for the **legitimate interests** of the School/Trust (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- o 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 1 of the special category conditions for processing under data protection law:

- o The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- o The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- o The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- o The data has already been made **manifestly public** by the individual
- o The data needs to be processed for the establishment, exercise or defence of **legal claims**
- o The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- o The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- o The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- o The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- o The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- o The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- o The data has already been made **manifestly public** by the individual
- o The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- o The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

## 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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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/Trusts record retention schedule outlined by the [Department for Education](#).

## 8. Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- o There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- o We need to liaise with other agencies – we will seek consent as necessary before doing this
- o 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 that can provide sufficient guarantees that they comply with UK data protection law
  - Establish a contract with the supplier or contractor 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
  - Carry out a Data Protection Impact Assessment (DPIA) which is to be reviewed by our DPO, where relevant (see section below).

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with UK data protection law.

## 9. Data Protection Impact Assessments (DPIA)

In order to achieve a privacy by design approach, the Trust will conduct DPIAs for any new high-risk technologies or programmes being used by the School which could affect the processing of personal data.

The Trust carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and

- For large scale, systematic monitoring of a publicly accessible area (for example, through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and

The risk mitigation measures in place and demonstration of compliance.

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

### **10.1 Subject access requests**

By law, individuals have a right to make a 'subject access request' to gain access to personal information that the School/Trust holds about them.

This includes:

- o Confirmation that their personal data is being processed
- o Access to a copy of the data
- o The purposes of the data processing
- o The categories of personal data concerned
- o Who the data has been, or will be, shared with
- o How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- o Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- o The right to lodge a complaint with the ICO or another supervisory authority
- o The source of the data, if not the individual
- o Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- o The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form they must immediately forward it to the Trust Governance Professional and Headteacher.

### **10.2 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. The Headteacher of the school may discuss the request with the child to take their views into account. Identification checks regarding the proof of the relationship to the child may be required.

### **10.3 Responding to subject access requests**

When responding to requests, we:

- o May ask the individual to provide 2 forms of identification
- o May contact the individual via phone to confirm the request was made
- o Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- o Will provide the information free of charge. (where significant administrative time is required, a nominal fee may be charged)
- o 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 (these timeframes continue to apply when the school is closed during holidays).

We may not disclose information for a variety of reasons, such as if it:

- o Might cause serious harm to the physical or mental health of the pupil or another individual
- o Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- o Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- o Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

### **10.4 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:

- o Withdraw their consent to processing at any time
- o Receive certain information about the data controller's processing activities
- o Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- o Prevent use of their personal data for direct marketing
- o Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- o Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- o Be notified of a data breach (in certain circumstances)
- o Make a complaint to the ICO
- o 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.

## 11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO's guidance](#) for the use of CCTV, and comply with data protection principles.

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 each School's DPO.

## 12. Photographs and videos

As part of our Trust /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 the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the School/Trust takes photographs and videos, uses may include:

- o Within school on notice boards and in school magazines, brochures, newsletters, etc.
- o Outside of school by external agencies such as the school photographer, newspapers, campaigns
- o Online on our School or Trust 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.

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. Parent/carers are requested to submit preferences for use of photographs and video use when joining the school.

## 13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Veritas MAT recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Veritas MAT will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

Veritas MAT will continue to review this policy in line with developments of AI within the education sector and any possible implementation of this across the Trust. Further detail can also be found in the Trust's Technical Security Policy on how the Trust aims to protect and safeguard the Trust from the use of AI.

## **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:

- o Appointing a suitably qualified Trust and School level DPOs, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- o 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)
- o Completing data protection impact assessments where the School/Trusts'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)
- o Integrating data protection into internal documents including this policy, any related policies and privacy notices
- o 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
- o Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- o Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- o Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our Schools / Trust and DPOs, 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, 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:

- o 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
- o Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- o Where personal information needs to be taken off site, staff must sign it in and out from the school office
- o Passwords should contain a mix of letters and numbers, which are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites, nor should passwords be shared with others.
- o Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- o Staff, pupils, Trustees 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 Technical Security Policy and acceptable use agreements).

- o 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. 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.

## 17. Personal data breaches

The School/Trust 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 after becoming aware of it. Such breaches in a school context may include, but are not limited to:

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

We will also notify the data subject where we are legally required to do so.

## 18. Complaints

We take any complaints about how we collect and use personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting the Trust Governance Professional ([governance.professional@veritasmat.co.uk](mailto:governance.professional@veritasmat.co.uk)) or via the Trust DPO.

Upon receiving a complaint, we will:

- o Acknowledge receipt of the complaint within 30 days of receiving it
- o Without undue delay, take appropriate steps to respond to the complaint, including:
  - o Making appropriate enquiries based on the circumstances of the complaint
  - o Keeping the complainant informed on the progress of the investigation
  - o Comparing the information from the complaint with the information you hold
  - o Checking you've upheld your own terms, policies and standards
- o Without undue delay, inform the complainant of the outcome of the investigation

## 19. Training

All staff, Trustees, Members 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.

## **20. Monitoring arrangements**

The Trust DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Trust Board.

## **21. Links with other policies**

This data protection policy is linked to our:

- o Freedom of information publication scheme
- o Child Protection and Safeguarding Policy

## Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach within a School, the staff member, governor or data processor must immediately notify the School's data protection officer (DPO) in writing, copying in the Governance Professional inbox. For Trust breaches of data, the Trust DPO (Judicium) must be notified in writing via the Governance Professional.
- The relevant DPO will liaise with the Governance Professional and 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
- Staff, Trustees and Governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the School DPO will alert the Headteacher, Trust Governance Professional and Trust DPO (via the Jedu platform). The Governance Professional will notify the CEO and Chair of Trust Board for any Trust wide breaches.
- The School / Trust DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPOs with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The Trust DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The Trust DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The Trust DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored securely by the Jedu platform.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the Jedu Platform, or ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 relevant 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 relevant DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons

why, and when the DPO expects to have further information. The relevant DPO will submit the remaining information as soon as possible

- Where the School/Trust is required to communicate with individuals whose personal data has been breached, the Trust DPO will provide guidance in advising them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the relevant 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 relevant DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The relevant 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 via a secure GDPR folder with restricted access to the School's DPO and Headteacher.

- For School breaches, the DPO, Trust DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. For the Trust, this meeting will include the Governance Professional, Trust DPO and CEO. This meeting will happen as soon as reasonably possible
- The Trust DPO will meet regularly with School DPOs to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches. School DPOs are encouraged to meet regularly with Headteachers to discuss this also.

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

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

For example:

### **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/external IT support provider] to attempt to recall it from external recipients and remove it from the School's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the School DPO will consider whether it's appropriate to 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 endeavor to obtain 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
- If safeguarding information is compromised, the DPO will inform the School Designated Safeguarding Lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners. The Trust Designated Safeguarding Lead should be informed.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families.