



# Data Protection Policy

Who is Responsible	VLT Finance and General Purposes Committee
Statutory Policy	Yes
Review Timescale	Annually
Approval date	15 <sup>th</sup> May 2018
Next Review	May 2019

## Contents

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

## 1. Aims

Our Academy aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [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 meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• 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.</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>• Political opinions</li><li>• Religious or philosophical beliefs</li></ul>

	<ul style="list-style-type: none"> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</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

Our Academies processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

##### 5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust 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 governing board and, where relevant, report to the board their advice and recommendations on Academy data protection issues.

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

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Ms A Britton and is contactable on [dposchools@somerset.gov.uk](mailto:dposchools@somerset.gov.uk)

## **5.3 Headteacher**

The Executive Headteacher acts as the representative of the data controller on a day-to-day basis.

## **5.4 All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy 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 Academies 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 Academy 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 Academy can **fulfil a contract** with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy 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 Academy, 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 Academy 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 apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

### 7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for Academics](#)

## 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 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 Academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned

- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, by either letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO.

### **9.2 Children and subject access requests**

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 below this age 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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils above this age may not 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.

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

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- 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 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 (where we have asked for consent to be given).
- 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)

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, are able to request access to their child's educational record (which includes most information about a pupil), by making a request in writing to the Academy.

## **11. Biometric recognition systems**

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use thumbprints to receive Academy dinners instead of paying with cash), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the Academy's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for Academy dinners using a pin number if they wish.

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

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

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

## **12. CCTV**

We use CCTV in various locations around the Academy sites 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 individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and there is prominent signage explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Academy Business Manager.

## **13. Photographs and videos**

As part of our Academy activities, we may take photographs and record images of individuals.

We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Uses may include:

- Within Academy on notice boards and in Academy magazines, brochures, newsletters, etc.
- Outside of Academy by external agencies such as the Academy photographer & newspapers
- Online on our Academy website or social media pages
- In filmed lessons used as learning resources

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will where practical, delete the photograph or video and not distribute it further.

## **14. Data protection by design and default**

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing privacy impact assessments where the Academy'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 Academy and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

## **15. Data security and storage of records**

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

In particular:

- Paper-based records 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 Academy computers, laptops and other electronic devices.
- Passwords must be kept confidential and changed immediately if there is a suspicion that they have been compromised.
- Encryption software is used to protect all portable devices such as laptops and smart phones.
- No personal data is to be stored on removable media such as USB memory devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our acceptable use agreements)
- 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. Retention and Disposal of records**

Records Management is the process by which the Trust and its Academies manage all aspects of any type of 'record' whether internally or externally generated and in any format or media type, from their creation, throughout their lifecycle and to their eventual disposal.

### 16.1. Relevant Data Protection Principles

The data protection principles, which directly relate to the management, retention and disposal of Personal Data are that the Personal Data must:

- I. be accurate and kept up to date (Principle 4)
- II. not be kept longer than necessary for the purpose for which it was obtained (Principle 5)
- III. be processed by a Data Controller who has in place appropriate technical and organisational measures to prevent unauthorised processing and accidental loss, destruction or damage (Principle 7).

### 16.2 Retention Periods

In line with the fifth principle as set out at 16.1 (ii) above each Academy and the Trust will not retain Data any longer than necessary and in determining an appropriate retention period will take into account the following:

- I. The current and future value of the Data.
- II. The costs, risks and liabilities associated with retaining the Data.
- III. The ease or difficulty in ensuring the Data remains accurate and up-to-date.

The standard default period for retaining Data will be based on the [Records Management Toolkit for Academics](#) produced by the Records Management Society. The retention schedule for the main types of data we hold within the Trust are set out in Appendix 1. A more comprehensive list can be seen in the toolkit.

### 16.3 Exceptions to the Retention Period

In the majority of cases, Data will be securely disposed of when it reaches the end of the retention period. When assessing whether Data should be retained beyond the retention period the Academy or the Trust will consider whether:

- The Data is subject to a request pursuant to the DPA.
- The Academy or the Trust is the subject of, or involved in ongoing legal action to which the Data is or may be relevant.
- The Data is or could be needed in connection with an ongoing investigation.
- There is a greater public interest in retaining the Data.
- There are changes to the regulatory or statutory framework.

#### 16.4 Disposal of Data

The destruction of Data is an irreversible act and must be clearly documented. All Data identified for disposal will be destroyed under confidential conditions.

The Academy or the Trust may sub-contract to another organisation its obligations to dispose of Data under confidential conditions. Where the obligation to securely dispose of Data is sub-contracted, the Academy or the Trust will satisfy itself of the subcontractor/third party's experience and competence to do so.

#### 16.5 Manual Records

Where Data is held in paper or other manual form, the retention period has expired and none of the exceptions for retaining Data beyond the retention period as set out at paragraph 16.3 is satisfied, the Academy or the Trust will ensure the Data is shredded or otherwise confidentially disposed of.

#### 16.7 Electronic Records

Where Data is held in an electronic format the Academy or Trust will, where feasible, use its reasonable endeavours to:

- I. Surround the Data with such technical and security measures to ensure it is not accessible other than by a Data Processor.

When the data is no longer required:

- II. Put the Data beyond use so that the Data is no longer on a live electronic system and cannot be accessed by its own employees (with the exception of IT support) or a Data Processor.
- III. Permanently delete the Data from the Academy electronic systems when and where this becomes possible.

Where the steps set out at paragraph 16.7.ii are complied with, the Academy considers the Data to be 'put beyond use' and this Data will not be used in order to respond to a Subject Access Request.

## **17. Personal data breaches**

The Academy 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 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an Academy context may include, but are not limited to:

- A non-anonymised dataset being published.
- Safeguarding information being made available to an unauthorised person.
- The theft of a Academy laptop containing non-encrypted personal data about pupils.

## **18. Training**

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy'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 Academy's practice. Otherwise, or from then on, this policy will be reviewed **every year by the Trust Finance and General Purposes Committee**.

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

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy Notice – Employees
- Privacy Notice – Parents
- Privacy Notice – Students
- Privacy Notice - Governance
- Acceptable Use Agreements – Employees
- Acceptable Use Agreement – Students
- CCTV Policy

## Appendix 1

The following retention schedule is in operation. This lays down the length of time a record needs to be retained, after which it will be destroyed. Time scales are based on local Government guidelines.

Students	Students' academic records, reports and IEPs	DOB of pupil + 25 years (records moved from Primary to Secondary Academy)
	Students attendance registers	Date of register + 3 years
	Exam results (internal & external)	Added to student file
	Statements of Special Needs	DOB + 30 years
	Child Protection Information	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.
	Timetable	Current Year + 1 Year
	Syllabus	Current Year + 1 Year
	Markbooks	Current Year + 1 Year
Students work*	Current Year + 1 Year  *It may be necessary to extend this period for examination work.	

Personnel	Staff Personnel Files	Termination of employment + 6 years
	Records leading to appointment of a new Headteacher	Date of appointment + 6 years
	Records leading to appointment of a new member of staff (unsuccessful candidates)	Date of interview + 6 months
	Pre-employment vetting	Date of check + 6 months
	Disciplinary proceedings	As specified
	Appraisal	Current year + 5 years

	Allegation of a child protection nature against a member of staff including where the allegation is unfounded	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned
--	---	--

Health and Safety	Accident reporting: Adults	Current year + 6 years
	Accident reporting: Children	DOB + 25 years
	Injury at work	Current year + 12 years then review
	Policy	Life of policy + 3 years
	Fire Log Books	Current year + 6 years
	Risk Assessments	Current year + 3 years
	COSHH Data	Current Year + 40 years
	Asbestos Monitoring	Current Year + 40 years

Senior Leadership Team	Minutes of meetings	Date of Meeting + 3 Years
	Reports created for SLT Meetings	Date of Meeting + 3 Years
	Academy Development Plans	Life of plan + 6 Years
	Academy Evaluation Forms	Life of plan + 6 Years

Directors / Governors	Minutes of Meetings	Permanent
	Agendas	Date of Meeting
	Reports presented to meetings	Date of meeting + 6 years
	Parental Complaints	Resolution + 6 years (then review before disposal)

	Admissions data	Date of Admission + 1 year
	Admissions Appeals	Date of hearing + 1 year

General	Prospectus	Current Year + 3 Years
	Newsletters	Current Year + 1 Year
	Visitors Book	Current Year + 6 Years
	OFSTED Reports	25 years
	Employers Liability Insurance	Closure of Academy + 40 years
	Maintenance Records	Current Year + 6 Years

Finance	PAYE & NI Returns	Current Year + 6 Years
	Pension Returns	
	Invoices	
	Remittance Advices	
	Bank Statements	
	Cheque Books	
	Bank Reconciliations	
	Petty Cash records	
	DFE Returns	
	Direct debits	
	Contracts	Until expiry + 6 years
	Budgets	Current year + 3 years
	Budget preparation	Current year + 3 years
	Property Title Deeds	Permanent
	Leases	End of lease + 6 years
	Annual Accounts	Current Year + 6 years
Letting Information	Current Year + 6 years	

## Appendix 2

### Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within our network storage system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- A record of all breaches will be retained.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible