Batley Multi Academy Trust

Data Protection Policy

Batley Multi Academy Trust

Approved by: Board of Trustees	**Ratified:** September 2023
Last reviewed: August 2023	**Next review due by:** September 2024
Reviewed by: Data Protection Officer	

Policy Statement

Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a Multi Academy Trust ("Trust"), we will collect, store and **process personal data** about our young people, workforce, parents/carers and others. This makes us a **data controller** in relation to that **personal data**.

Batley Multi Academy Trust is registered as a data controller with the ICO (registration number: ZA421233) and will renew this registration annually or as otherwise legally required.

We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

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.

All members of our **workforce** must comply with this policy when processing **personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

About this Policy

The types of **personal data** that we may be required to handle include information about young people, parents/carers, our **workforce**, and others that we engage 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**').

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.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

Definition of Data Protection Terms

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

Data Protection Officer

As a Trust, we are required to appoint a Data Protection Officer ("DPO"). Our DPO is Laura Bland and they can be contacted at dpo@batleymat.co.uk.

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.

The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

Data Protection Principles

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

- **Processed** fairly and lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- **Processed** securely using appropriate technical and organisational measures.

Personal Data must also:

- be **processed** in line with **data subjects'** rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

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

Fair and Lawful Processing

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.

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

- that the **personal data** is being **processed**;
- why the **personal data** is being **processed**;
- what the lawful basis is for that **processing** (see below);
- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

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**.

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:

- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
- where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011);
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

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 dat**a under following legal grounds:

- where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
- where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- 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**.

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.

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

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

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.

There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

When our young people and/or our workforce join the Trust, a consent form will be required to be completed in relation to them. This consent form covers the taking and use of photographs and videos of them. Where appropriate third parties may also be required to complete a consent form.

In relation to all our young people under the age of 18 years old we will seek consent from an individual with parental responsibility for that young person.

We will generally seek consent directly from a young person who has reached the age of 18 or above, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

- Inform the **data subject** of exactly what we intend to do with their **personal data**
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- Inform the **data subject** of how they can withdraw their consent.

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.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

Processing for Limited Purposes

In the course of our activities as a Trust, we may collect and **process** the **personal data.** This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents/carers, other young people or members of our **workforce**).

We will only process **personal data** for specific purposes or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

Notifying Data Subjects

If we collect **personal data** directly from **data subjects**, we will inform them about:

- our identity and contact details as **Data Controller** and those of the DPO;
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to our Retention Policy;
- 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
- 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.

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.

Accurate Data

We will ensure that **personal data** we hold is accurate and kept up to date. We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

Timely Processing

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.

We shall seek to comply with the rights exercised by **data subjects** as set out 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.

Processing in line with Data Subjects' Rights

We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

- request access to any **personal data** we hold about them;
- object to the **processing** of their **personal data**, including the right to object to direct marketing;
- have inaccurate or incomplete **personal data** about them rectified;
- restrict **processing** of their **personal data**;
- have **personal data** we hold about them erased
- have their **personal data** transferred; and

- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

Data subjects may request access to **personal data** we hold about them. This is called a Subject Access Request (SAR). If you would like to exercise this right, please contact the DPO.

Personal data about a child belongs to that child and not the child's parents/carers. For a parent/carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent.

Primary School
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents/carers may be granted without the express permission of their child. This is not a rule and a young person's ability to understand their rights will always be judged on a case-by-case basis.

Secondary School
Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents/carers may not be granted without the express permission of their child. This is not a rule and a young person's ability to understand their rights will always be judged on a case-by-case basis.

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 (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge. However, we can impose a charge for this information if the request is manifestly unfounded or excessive.
- 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 young person or another individual.
- 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.
- Would include another person's personal data that we can't reasonably anonymise, we don't have the other person's consent and it would be unreasonable to proceed without it.

- 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.
- Any other relevant exemption.

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. 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 SAR through the courts.

The DPO may need to carry out SAR searches linked to your school/Trust email account and/or documents held on school/Trust devices, cloud based systems and other platforms used relevant to your role. This will be done in line with data protection legislation.

The Right to Object

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.

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**.

Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

In respect of direct marketing any objection to **processing** must be complied with.

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

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.

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.

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

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.

The Trust must restrict the **processing** of **personal data**:

- Where it is in the process of considering a request for **personal data** to be rectified (see above);
- Where the Trust is in the process of considering an objection to processing by a **data subject**;
- Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and
- 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.

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. The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

Data subjects have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

- Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
- 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;
- 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;
- Where the **processing** of the **personal data** is otherwise unlawful;
- When it is necessary to erase the personal data to comply with a legal obligation; and

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:

- To exercise the right of freedom of expression or information
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
- For public health purposes in the public interest
- For archiving purposes in the public interest, research or statistical purposes
- In relation to a legal claim.

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. The DPO must be consulted in relation to requests under this right.

Right to Data Portability

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 another organisation. If such a request is made then the DPO must be consulted.

Data Security

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**.

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.

Security procedures include:

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported to a member of the school's Senior Leadership Team, or the CEO in relation to the Trust building immediately.
- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
- **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock their PC/log off from their PC when it is left unattended.
- **Working away from the school/Trust premises – paper documents.** Subject to the content of documents you are taking off-site you will be expected to complete the signing in/out form to detail this information.
- **Working away from the school/Trust premises – electronic working**. Online training will be provided to staff regularly and they should be aware of the safety protocols the Trust has in place with regards to working off-site from school or Trust premises. USB storage devices are not permitted in our Trust and information needed to work away from the school/Trust premises must not be stored on a USB device.
- **Document printing** - Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

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

Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the event of a suspected or actual 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 may include, but are not limited to:

- A non-anonymised dataset being published on the school/Trust website
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about young people.

The Trust is within its right to apply relevant HR related policies to the workforce if a data breach is considered significant, severe and/or they have repeatedly been involved in and/or caused data breaches.

Data Protection Impact Assessments

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.

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.

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

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

Disclosure and Sharing of Personal Information

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.

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.

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

Data Processors

We contract with various organisations who provide services to the Trust. In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

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 undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

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**.

Images and Videos

Parents/carers and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents/carers can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

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.

The Trust asks that parents/carers 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.

As a Trust we want to celebrate the achievements of our young people and therefore may want to use images and videos of our young people within promotional materials, or for publication in the media such as local, or even national, newspapers covering school/Trust events or achievements. We will seek the consent of young people, and their parents/carers where appropriate, before allowing the use of images or videos of young people for such purposes.

Whenever a young person begins their attendance at a Trust school they, or their parent/carer, where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that young person. We will not use images or videos of young people for any purpose where we do not have consent.

Video Surveillance

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

Biometric Data

Within our Trust we operate a biometric recognition system for the purposes of payment of dinner monies.

Before we are able to obtain the Biometric Data of young people, or the workforce, we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

For the relevant workforce, written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of their Biometric Data is received from the individual.

For young people under the age of 18 years, the relevant school will notify each parent/carer of that young person (that the school has the contact details for and is able to contact) prior to them commencing their education at the school of the use of our Biometric Recognition System. The school will then obtain the written consent of one of the young person's parents/carers before obtaining any Biometric Data.

In the event that written consent cannot be obtained from a parent/carer, or any parent/carer objects in writing, or the young person objects or refuses to participate in the processing of their Biometric Data, the school will not process the young person's Biometric Data and will provide an alternative means of accessing the above services (e.g a PIN).

Further information about this can be found in our Biometric Data Consent Form and our Privacy Notices.

Changes to this Policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Appendix 1 - 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	is a system that operates automatically (electronically) and : • Obtains or records information about a person's physical or behavioural characteristics or features; and • 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
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 young persons, 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 Trustees, 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 Members, Trustees, Governors, parent/carer helpers.

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 necessary individuals within school and the Trust.
- 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 and the individuals affected using the ICO's self-assessment tool. This must be judged on a case-by-case basis.
- 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 on each school's breach log.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113) 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:

  - A description, in clear and plain language, of the nature of the personal data breach.
  - 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.

- As above, any decision on whether to contact individuals will be documented by the DPO.

- 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).

- The DPO, Headteacher and where relevant, SLT and/or Trust CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Special category data (sensitive information) being disclosed via email (including safeguarding records)

If special category data 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.

Staff are expected to set a 30 second recall/undo period on their emails. For information on how to do this, please click here.

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 IT department to recall it.

In any cases where the recall is unsuccessful, the DPO (or delegated member of staff) will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The DPO (or delegated member of staff) will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.