PROSPER TOGETHER
MULTI ACADEMY TRUST

DATA PROTECTION POLICY

DATE	PREPARED BY	REVIEW DATE
DEC 2025	DPO	DEC 2028

Contents

Prosper Together Multi Academy Trust (the 'Trust') refers to all the Trust member schools and the central team.

Data Protection Policy

1. Aims

Prosper Together Multi Academy Trust (the '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.

2. Legislation and Guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Data Use and Access Act 2025 (DUAA)
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- Privacy and Electronic communications Regulations 2003 (PECR)
- Article 8 of the Human Rights Act 1998

It is based on guidance published by the Information Commissioner's Office (ICO) and guidance from the Department for Education (DfE)

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
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

TERM	DEFINITION
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	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 processes personal data relating to parents and carers, pupils, staff, trustees, governors, visitors and others, and therefore is a data controller.

The Trust is registered with the Information Commissioner's Office (ICO), as legally required. Our registration number is: ZB533652

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 Trust Board

The Trust Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

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 school data protection issues.

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

The Trust's DPO is provided by Services 4 Schools Ltd and can be contacted by:

Email – DPO@ptmat.org

Or by post –

FAO:The Data Protection Officer
Prosper Together Multi Academy Trust
c/o Fordbridge Community Primary School
Crabtree Drive,
Fordbridge,
Birmingham
B37 5BU

Each school has a nominated Data Protection Lead (DPL) that oversees the day-to-day management of day protection within the school setting. Details of individual school Data Protection Leads are available at Appendix A.

5.3 Head Teacher

The Head Teacher 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 school of any changes to their personal data, such as a change of address.
- Only using personal data for the purposes identified in Privacy Notices, or a lawful purpose that has been authorised by the Trust.
- Contacting the DPO in the following circumstances:
    - If they are concerned that a data breach has occurred,
    - If they receive a request from an individual wishing to exercise their information rights (such as a subject access request)
    - 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.
- 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 the Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

The Trust will only process personal data where there is 1 of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone’s life.
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority.**
- The data needs to be processed for the **legitimate interests** of the school (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.

- The data is needed for **recognised legitimate interests** by an Official Body for a statutory purpose, or linked to regulatory activity (such as the Police in the undertaking of their duties, or a Local Authority for the investigation of fraudulent activities)
- 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, the Trust will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent.**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law.**
- 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.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- 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.
- 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.
- 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, the Trust will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent.**
- 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.
- The data has already been made **manifestly public** by the individual.
- 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.**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

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

This will usually be done in the form of a Privacy Notice published on the Trust or relevant school's website.

The Trust will always consider the fairness of its data processing. It will ensure it does 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

The Trust will only collect personal data for specified, explicit and legitimate reasons. The reasons will be explained to the individuals when the data is first collected.

If the Trust wants to use personal data for reasons other than those given when it was first obtained, the individuals concerned will be informed before the Trust does so, and consent will be sought where necessary.

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

The Trust 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 Trust's Record Management Policy and Retention Schedule.

8. Sharing Personal Data

The Trust will not normally share personal data with organisations not referenced in its Privacy Notices, but there are certain circumstances where it may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of Trust staff at risk.
- There is a statutory or regulatory need to liaise with other agencies
- Suppliers or contractors need data to enable the Trust to provide services to its staff and pupils – for example, IT companies. When doing this, the Trust 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.

The Trust will also share personal data with law enforcement and government bodies where it is legally required to do so.

The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation, which affects pupils or staff.

Where the Trust transfers personal data internationally, it will do so in accordance with UK data protection law.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- 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.
- 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:

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

If staff receive a subject access request in any form they must immediately forward it to the DPL in school and inform 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 at any of the Trust schools 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. If the Trust deem that a parent/carer is not acting in the interests of the child, the request may be refused.

9.3 Responding to Subject Access Requests

When responding to requests, the Trust:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- May require that the request is clarified before proceeding, if the scope of the request is not clear and the types or records, or relevant time periods have not been specified.
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, or further clarification where relevant).
- Will provide the information free of charge, unless the duplicate copies of information are requested, or the request is deemed to be manifestly excessive.
- May tell the individual it will comply within 3 months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within 1 month, and explain why the extension is necessary.

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

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is subject of a safeguarding concern, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that cannot be reasonably anonymised, and it does not 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.

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

When the Trust refuses a request, it 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.

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 the Trust is collecting their data about how it will be used and processed (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests.
- 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).
- 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 DPL and inform the DPO.

10. Parental Requests to see the Educational Record

Parents, or those with parental responsibility, may access to their child's educational record (which includes most information about a pupil) within 20 school days of receipt of a written request, without a charge.

If the request is for a copy of the educational record, the Trust may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric Recognition Systems

Where the Trust uses pupils' biometric data as part of an automated biometric recognition system (for example, to administer library services), we will comply with the requirements of the Protection of Freedoms Act 2012 (please note a 'child' under the Act is a person aged under 18 years of age).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before it takes any biometric data from their child and first processes it.

Parents/carers and pupils have the right to choose not to use the school's biometric

system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and the Trust 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, the Trust 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 a school'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 school will delete any relevant data already captured.

12. CCTV

The Trust uses CCTV in various locations around school sites to ensure it remains safe. The Trust operates a CCTV policy which is based on the ICO's guidance for the use of CCTV, and complies with data protection principles.

The Trust does not need to ask individuals' permission to use CCTV, but will 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 on a school site should be directed to the school office.

13. Photographs and Videos

As part of the Trust and school activities, schools may take photographs and record images of individuals within the school.

The Trust/school will obtain written consent from parents/carers for photographs and videos to be taken of their child for external communication, marketing and promotional materials. The Trust/school 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, the Trust/school 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 Trust/School takes photographs and videos, uses may include:

- For identification an safeguarding purposes, held in in our management information systems
- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on school/Trust website or social media pages

When using photographs and videos in this way no other personal information about the

child will accompany the photograph/video, to ensure they cannot be identified.

Please see the school specific child protection and safeguarding policy for more information on our use of photographs and videos.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Prosper Together Multi Academy Trust 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 personal data into generative AI tools or systems which process data using AI technologies that have not been authorised by the Trust.

Before using any AI technologies, the Trust will assess the associated data protection compliance risks.

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

15. Data protection by Design and Default

The Trust will put measures in place to show it has integrated data protection into all of its data processing activities, including:

- Appointing a 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 data protection impact assessments where the Trust'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; the Trust will also keep a record of attendance.
- Regularly conducting reviews and audits to test privacy measures and make sure the Trust is compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of the school and DPL/DPO, and all information we are required to share about how the School/Trust uses and processes their personal data (via privacy notices).
- For all personal data that the Trust holds, maintaining an internal record of the type of data, type of data subject, how and why the data is being used, 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.

16. Data Security and Storage of Records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Portable storage devices and removeable hard drives are not permitted for use at schools in the Trust.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.
- Staff are not permitted to transfer the personal data of pupils to personal devices without the permission of a Headteacher, or member of SLT.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see Trust and individual school online safety policy / acceptable use agreement / Mobile phone policy).
- Where the Trust needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

17. 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 the Trust cannot or does not need to rectify or update it.

For example, paper-based records will be shred or incinerated, and electronic files overwritten or deleted. The Trust may also use a third party to safely dispose of records

on its behalf. If this is actioned, the Trust will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, it will follow the procedure set out in appendix 1.

When appropriate, it 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:

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

19. Training

Relevant 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 Trust's processes make it necessary.

20. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

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

21. Complaints

If you have a complaint about how your personal data has been handled by Prosper Together Multi Academy Trust, you should contact the Data Protection Officer in the first instance.

This policy does not outline the process for complaints and concerns which are directly related to the processing of personal data. Please see the Trust Complaints policy if you have a complaint or concern which relates to another matter:
https://www.prospertogethermat.org/page/?title=Policies+%26amp%3B+Procedures&pid=22

Complaints or concerns which relate to data protection or information rights should be submitted in writing to DPO@ptmat.org

The Trust will conduct an internal review and respond to you within a calendar month.

If you are unsatisfied with the response the Trust has provided, you have the right to contact the Information Commissioners Office. You can do this online at:

https://ico.org.uk/make-a-complaint/your-personal-information-concerns/

22. Links with Other Policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Cyber Security Policy

Appendix A

School Data Protection Leads

SCHOOL NAME	NAME	ROLE	EMAIL
Castle Bromwich Infant and Nursery School	Hayley Dainty	Business Manager	office@cbins.solihull.sch.uk
Castle Bromwich Junior School	Julie Whitehouse	Business Manager	office@cbjs.solihull.sch.uk
Fordbridge Community Primary School	Elaine Robertson	Business Manager	office@fordbridge.solihull.sch.uk
Kingshurst Primary School	John Bousfield	Business Manager	34office@kingshurst.solihull.sch.uk
Windy Arbor Primary School	Fay Roper	Business Manager	office@windy-arbor.solihull.sch.uk

Appendix B

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, the staff member, trustee, governor or data processor must immediately notify the data protection officer (DPO) by emailing the Data Protection Breach form.
- 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
- Staff 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 DPO will alert the Head Teacher and the Chair of Governors in the school and/or the Chief Executive Officer and Chair of Trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO 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 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 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 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 in the secure area of the PTMAT Drive.
- Where the ICO must be notified, the DPO will do 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 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 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 DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell 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 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 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 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 on the PTMAT Drive.

- The DPO and Head Teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPO and Head Teacher will meet bi-annually to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

The Trust will review the effectiveness of any actions taken to minimise the impact of a data breach and amend them as necessary after any data breach.

The DPO will also record and review near misses.

Example actions:

- 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.
- The DPO will endeavour 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 designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners.