Midsomer Norton Schools Partnership

Issued: March 2025
Review: Term 1 annually
LST: CHO

DATA PROTECTION and DATA BREACH POLICY

Contents

1. Aims

The Midsomer Norton Schools' Partnership (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) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

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

- All Schools that use biometric data meet the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- All Schools that use CCTV reflect the ICO's guidance for the use of surveillance cameras and personal information. Please refer to the Trust CCTV Policy.
- This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.
- 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.
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.

TERM	DEFINITION
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

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

The Trust and all our schools are registered with the ICO, as legally required.

5. Roles and responsibilities

This policy applies to all staff employed by the Midsomer Norton Schools' Partnership 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 schools comply 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 Trust 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.

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

Our DPO for the Trust is Chris Hobbs and is contactable via email - headoffice@msnpartnership.com or by contacting the Head Office:

Midsomer Norton Schools Partnership Head Office, Knobsbury Lane, Writhlington, Radstock, BA3 3NQ / 01761 205628

5.3 Headteacher

The headteacher at each school site will act 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;
- 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 UK;

➔ If there has been a data breach;

➔ Whenever they are engaging in a new activity that may affect the privacy rights of individuals;

➔ If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles that our Trust and all schools 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 Trust and associated schools aim to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency
We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust/School can **fulfil a contract** with the individual, or the individual has asked the Trust/School to take specific steps before entering into a contract;
- The data needs to be processed so that the Trust/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 Trust/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 Trust/School (where the processing is not for any tasks the Trust/School performs as a public authority) 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 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, we 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 we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

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

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

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

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we 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 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, Educational Welfare Officers, etc. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law;
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share;
    - Only share data that the supplier or contractor needs to carry out their service.

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

9. 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;

Please refer to the Trust Subject Access Request Policy and associated form.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request*.

This will be provided electronically in the first instance, if the request is for a hard copy of the educational record, the school 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.

**The Trust supports the parental right of access to educational records from our schools.*

11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school 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 Trust/school will get written consent from at least 1 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 biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, a till operative will manually search for a pupil record and can then record the transaction.

Parents/carers and pupils can 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 Trust/School 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 Trust/School will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the Trust to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

For further information please refer to the Trust CCTV Policy

13. Photographs and videos

As part of the Trust schools activities, we may take photographs and record images of individuals within our Trust/School systems.

In all our **Trust Schools** we will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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

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

- Within Trust/School on notice boards and in school promotional materials, brochures, newsletters, etc.
- Outside of Trust/School by external agencies such as the school photographer, newspapers, campaigns.
- Online on our Trust/School website or social media pages.

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

For further information please refer to the Trust Photographs of Pupils Policy

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The 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 data into unauthorised generative AI tools or chatbots.

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

For further information please refer to the Trust AI Policy

15. 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 data protection impact assessments where the school'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.
- 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 our Trust and DPO, and all information we are required to share about how we use and process their personal data (via our Fair Processing Notices Parents & Students and School Workforce).
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure..

16. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are at least 10 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.
- Encryption software is used to protect all portable devices and removable media, such as laptops/chrome books.
- Staff, pupils and governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.

For further information please refer to the Trust IT Acceptable User Policy for Adults and Students

- 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).

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 we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- 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

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 Trusts processes make it necessary.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually in Term 1 and approved by the full Trust board.

21. Links with other policies

This Policy should be read in conjunction with other Trust Policies available on the Trust website:

- AI
- CCTV
- Child Protection & Safeguarding
- Code of Conduct
- Examinations
- Fair Processing
- Freedom of information
- ICT AUP
- Internet Filtering
- Mobile Devices AUP
- Online Safety
- Photographs of Pupils
- Records Retention
- Subject Access Requests

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by Completing and submitting the Data Breach Form Appendix 2.
- 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 cooperate 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 headteacher and this should be communicated to the schools chair of governors.
- 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 relevant folder of google drive.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out::
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned.
    - The categories and approximate number of personal data records concerned.
  - The name and contact details of the 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 in the central google folder set up for this purpose.

- 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.

- The DPO and CEO will meet regularly 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 following steps should be reviewed to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender, their headteacher 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 Trust ICT department or external IT contractor to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

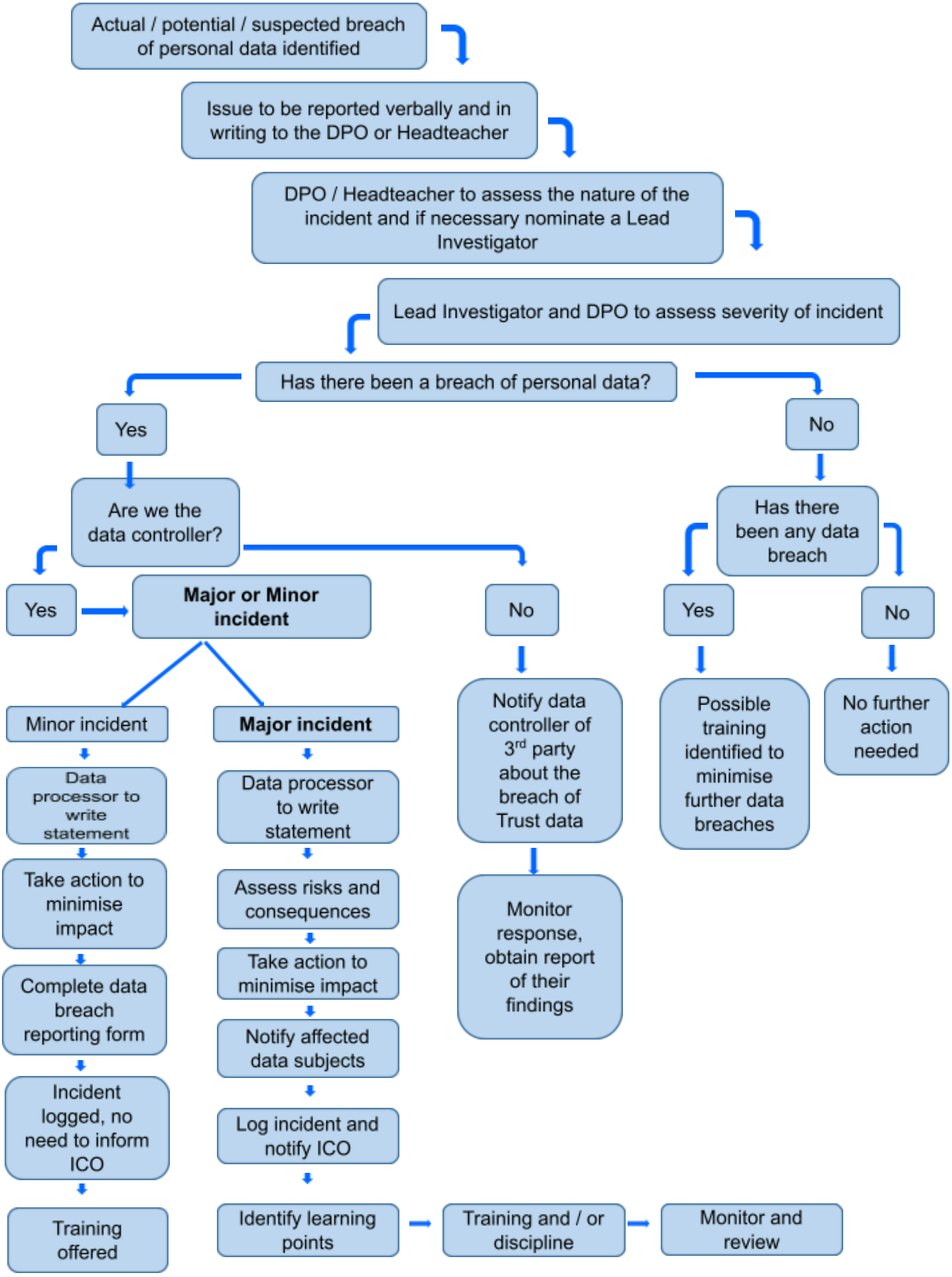
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the Trust/School should inform any, or all, of its local safeguarding partners.

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- Hardcopy reports sent to the wrong pupils or families

Data Breach Flow Diagram



Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your Headteacher immediately, who will then inform the DPO.

Download a copy of this form and complete Section 1 and Section 2 and share it with your Headteacher who will complete Section 3. The completed form should be emailed to the Trust Data Protection Officer - chobbs@msnpartnership.com

Section 1 - Notification of Data Security Breach

Name of person reporting the incident	
Position / Role	
Date form completed	
Contact details of person reporting incident (email, and phone number including any extension)	

About the incident

Date and time incident discovered	
Date and time incident occurred	
Place of incident	
How were you made aware of the data incident and by whom?	
Brief description of incident or details of the information lost	
Number of data subjects affected (if known)	
Has any personal data been placed at risk? If so, give full details of the type of data?	
Brief description of action taken when the incident was discovered?	

Section 2 - Assessment of Severity

Details of the IT systems, equipment, devices, records etc. involved in the security breach:	

Details of information loss:

Type of Breach (Please select)	Human error	System breakdown	Theft	Deleted or altered data	Lost (eg. laptop)
Category of Impact (Please select)	Confidentiality		Integrity		Availability
Level of risk (Please select)	High* ***Breach may have considerable impact on affected individuals.**		Medium* ***Breach may have an impact on individuals, but the impact is unlikely to be substantial.**		Low* ***The breach is unlikely to have an impact and/or impact is likely to be minimal.**

Lost Data

What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop last connected to the internet or local school network?	
Is the information unique? Will its loss have adverse operational, financial legal, liability or reputational consequences for the Trust or third parties?	

High Risk Data (please complete if relevant)

Please provide details of any types of information that fall into the high risk category:	
HIGH RISK personal data **Special categories personal data** *(as defined in the Data Protection Legislation)* relating to living, identifiable individuals. ● Racial or ethnic origin; ● political opinions or religious beliefs; ● trade union membership; ● genetics; ● biometrics (where used for ID purposes) ● health; ● sex life or sexual orientation.	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	

Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
Security information that would compromise the safety of individuals if disclosed.	

Implications of the breach

To be completed by the staff member reporting the breach

Completed by:	Name:	Role:
Date sent to Headteacher:		

Section 3 - Actions Taken

To be completed by the Headteacher in consultation with the Trust DPO.

Actions taken to reduce the impact of the breach - What measures were taken at the time? If data subjects were made aware please give details of who and how they were informed.

Other follow up actions required - What has been done since? e.g. staff retraining? whole school awareness etc? Change of procedure. Please give details and timescales.

To be completed by Headteacher

Completed by:	
Signature:	
Date sent to DPO:	

Section 4 - Notification *(To be completed by the DPO)*

Is this a notifiable breach to the ICO	Yes	No
If reported to the ICO, Please give a date.		

Reasons for decision about notifying the ICO

Was the incident reported to police? If so, date and crime number?	
Have data subjects been informed about the incident? If Yes, state method used and date.	
Notified to other external agencies? If Yes, date and reason.	

Notifications (apart from the ICO, who else needs to be notified?)

DPO Recommendations

What lessons can be learnt from this incident?

Is there a training (re-training) requirement

To be completed by DPO

Name of DPO:	Chris Hobbs
Signature:	
Date approved:	