Data Protection Policy

March 2023

Review date: March 2025

Data Protection Policy

Contents

1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as an Academy Trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

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

1.3 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.

1.4 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.

2 About this policy

The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in 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').

2.1 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.

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

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

3 Definition of data protection terms

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

4 Data Protection Officer

4.1 As a Trust we are required to appoint a Data Protection Officer ("DPO"). Our DPO is SBM Services Ltd, and they can be contacted by email at dpo@sbmservices.co.uk or by calling their helpdesk on 01206 671103.

4.2 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.

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

5 **All Trust and academy staff must**

5.1 Familiarise themselves and comply with the Data Protection Policy.

5.2 Comply with the Trust data protection arrangements.

5.3 Follow the data breach reporting process.

5.4 Attend data protection training as organised by the Trust/school.

6 **Data protection principles**

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

6.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**;

6.1.2 **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;

6.1.3 Adequate, relevant and not excessive for the purpose;

6.1.4 Accurate and up to date;

6.1.5 Not kept for any longer than is necessary for the purpose; and

6.1.6 **Processed** securely using appropriate technical and organisational measures.

6.2 **Personal Data** must also:

6.2.1 be **processed** in line with **data subjects'** rights;

6.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

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

7 **Fair and lawful processing**

7.1 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**.

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

7.2.1 that the **personal data** is being **processed**;

7.2.2 why the **personal data** is being **processed**;

7.2.3 what the lawful basis is for that **processing** (see below);

7.2.4 whether the **personal data** will be shared, and if so with whom;

7.2.5 the period for which the **personal data** will be held;

7.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and

7.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

7.3 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**.

7.4 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:

7.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

7.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);

7.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and

7.4.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

7.5 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 data** under following legal grounds:

7.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

7.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

7.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

7.5.4 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**.

7.6 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.

7.7 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

7.8 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

7.9 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.

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

7.11 When pupils and or our Workforce join the Trust and/or Academy a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

7.12 In relation to all pupils under the age of 12/13 years old we will seek consent from an individual with parental responsibility for that pupil.

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

7.13.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

7.13.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

7.13.3 Inform the **data subject** of how they can withdraw their consent.

7.14 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.

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

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

8 Processing for limited purposes

8.1 In the course of our activities as a Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for

example, local authorities, other schools, parents, other pupils or members of our **workforce**).

8.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

9 Notifying data subjects

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

9.1.1 our identity and contact details as **Data Controller** and those of the DPO;

9.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**;

9.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;

9.1.4 whether the **personal data** will be transferred outside the European Economic Area ('**EEA**') and if so the safeguards in place;

9.1.5 the period for which their **personal data** will be stored.

9.1.6 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

9.1.7 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.

9.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

9.3 The Trust will be provided with information relating to third parties in the form of emergency contact details. These individuals must be provided with the information above. Parents are required to obtain the consent of any third party whose details they provide to the Trust or Academy/School for these purposes.

10 Adequate, relevant and non-excessive processing

10.1 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.

11 **Accurate data**

11.1 We will ensure that **personal data** we hold is accurate and kept up to date.

11.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

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

12 **Timely processing**

12.1 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.

12.2 We shall seek to comply with the rights exercised by **data subjects** as set out in section 12 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 till be notified and provided details about the reason for the delay and when a response can reasonably be expected.

13 **Processing in line with data subject's rights**

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

13.1.1 request access to any **personal data** we hold about them;

13.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

13.1.3 have inaccurate or incomplete **personal data** about them rectified;

13.1.4 restrict **processing** of their **personal data**;

13.1.5 have **personal data** we hold about them erased

13.1.6 have their **personal data** transferred; and

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

The Right of Access to Personal Data

13.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure below:

13.2.1 All staff, parents and other users are entitled to know what data about them or their child is being processed and be able to access such data, should they wish.

13.2.2 Anyone wishing to exercise this right should submit the Subject Access request (SAR) verbally or in writing and submit it to the DPO. Any staff receiving a request which could be considered a SAR should pass it on immediately to the DPO.

13.2.3 For processing SAR's, is free of charge however if a request is manifestly unfounded or excessive e.g. repetitive then a reasonable fee maybe charged.

13.2.4 Subject Access requests will be processed as quickly as possible, and the required information will be supplied in permanent form (either physical or electronic) within 1 month. Proof of identity may be required before the information is released.

13.2.5 When supplying data in response to a SAR, data relating to third parties must be anonymised, unless consent has been obtained from the third party for such disclosure.

13.2.6 If for any reason the required information cannot be provided within one month, the reason will be explained in writing to the individual making the request.

The Right to Object

13.3 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.

13.4 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**.

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

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

13.7 The Trust or Academy 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

13.8 If a **data subject** informs the Trust or Academy that **personal data** held about them by the Trust or Academy is inaccurate or incomplete then we will consider that request and provide a response within one month.

13.9 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.

13.10 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

13.11 **Data subjects** have a right to "block" or suppress the **processing** of **personal data**. This means that the Trust or Academy can continue to hold the **personal data** but not do anything else with it.

13.12 The Trust or Academy must restrict the **processing** of **personal data**:

13.12.1 Where it is in the process of considering a request for **personal data** to be rectified (see above);

13.12.2 Where the Trust or Academy is in the process of considering an objection to processing by a **data subject**;

13.12.3 Where the **processing** is unlawful but the **data subject** has asked the Trust or Academy not to delete the **personal data**; and

13.12.4 Where the Trust or Academy no longer needs the **personal data** but the **data subject** has asked the Trust or Academy not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust or Academy.

13.13 If the Trust or Academy 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.

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

The Right to Be Forgotten

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

13.15.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected;

13.15.2 When a **data subject** withdraws consent – which will apply only where the Trust or Academy is relying on the individuals consent to the **processing** in the first place;

13.15.3 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;

13.15.4 Where the **processing** of the **personal data** is otherwise unlawful;

13.15.5 When it is necessary to erase the **personal data** to comply with a legal obligation

13.16 The Trust or Academy/School is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

13.16.1 To exercise the right of freedom of expression or information;

13.16.2 To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;

13.16.3 For public health purposes in the public interest;

13.16.4 For archiving purposes in the public interest, research or statistical purposes; or

13.16.5 In relation to a legal claim.

13.17 If the Trust or Academy 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.

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

Right to Data Portability

13.19 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 other organisation.

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

14 Data security

14.1 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**.

14.2 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.

14.3 Security procedures include:

14.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the main school office.

14.3.2 **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.)

14.3.3 **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.

14.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

14.3.5 **Working away from the school premises – paper documents.** Personal information should not be removed from site. Children's books should not include dob or year groups.

14.3.6 **Working away from the school premises – electronic working.** Information is only to be stored on the one drive.

14.3.7 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

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

15 Data Protection Impact Assessments

15.1 The Trust & Academy 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.

15.2 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.

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

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

16 Disclosure and sharing of personal information

16.1 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, and / or 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.

16.2 The Trust or Academy 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.

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

17 Data Processors

17.1 We contract with various organisations who provide services to the Trust or Academy, including:

17.1.1 Payment processing, communication, medical training, performance management, Attendance, School Meal Providers

17.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

17.3 **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 & Academy. The Trust & Academy will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

17.4 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**.

18 Images and Videos

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

18.2 The Trust & Academy 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 & Academy to prevent.

18.3 The Trust & Academy asks that parents 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.

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

18.5 Whenever a pupil begins their attendance at the Trust & Academy they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18.6 Images of staff may be published without consent and any staff who wish not to have their images published should speak to a designated data controller.

19 Video Surveillance

19.1 CCTV footage must be handled in line with the Data Protection Principles and therefore staff must ensure that:

19.1.1 Staff, pupils and visitors are notified of the purpose of collecting and processing CCTV footage, either by way of the Data Protection Code of Practice or visible signage

19.1.2 Cameras are sited only where necessary and do not intrude on people's privacy

19.1.3 Footage is retained for no longer than one month and completely destroyed after this time period

19.1.4 Access to footage is granted on a 'need to know' basis

20 Data Breaches

20.1 Although the Trust/school takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the Trust/school

20.2 The Trust has a Data Breach Procedure which sets out the process that should be followed in the event of a data breach occurring (Appendix B).

21 Changes to this policy

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

22 Approval and Review

This policy has been approved by the Board in March 2023.

This policy shall be reviewed no less than once every two years to ensure its continued effectiveness and compliance with the law and regulations.

Next review date: March 2025.

Appendix A

DEFINITIONS

Term	Definition
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 pupils, 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 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 the Trust such as staff and those who volunteer in any capacity including Governors / Trustees / Members/ parent helpers.

Appendix B

Data Breach Procedure (including 'near misses')

Although the Trust/school takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the Trust/school

However the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified that the breach has occurred must inform the Head of School who will notify the Senior Office Manager and the Trust DPO – SBM Services Ltd. They can be contacted by email at dpo@sbmservices.co.uk or by calling their helpdesk: 01206 671103.

2. A **record of the breach** should be created by the individual who has identified the breach using the template included in this document. The Senior Office Manager will maintain a log of all breaches across the Trust.

3. **Containment:** DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

4. **Recovery:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

5. **Assess the risks:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded by the Senior Office Manager in the Trust's Data Breach log:

    a. What type of data is involved
    b. How sensitive is it?
    c. If data has been lost/stolen, are there any protections in place such as encryption?
    d. What has happened to the data?
    e. What could the data tell a third party about the individual?
    f. How many individuals data have been affected by the breach?
    g. Whose data has been breached?
    h. What harm can come to those individuals?
    i. Are there wider consequences to consider such as reputational loss?

6. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

   The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

7. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the Trust/school.

8. **Evaluation:** The DPO should assess whether any changes need to be made to the Trust/ school processes and procedures to ensure that a similar breach does not occur.

Data Breach (including 'near misses') Incident Form

Data Breach Information:	
When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	
Data Breach Risk Assessment:	
What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	
Whose data has been breached:	

What harm can come to those individuals:	
Data Breach Notification:	
Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	
Data Breach Action Plan:	
Action to be taken to recover the data:	
Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	