Data Protection Policy

July 2026

Review date: July 2028

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**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data**. This policy sets out how we comply with the relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.

1.4 All data users must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

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 informing and advising the Trust about data protection legislation, 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, the Information Commissioner's Office ("ICO")** 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 Our data protection commitments

6.1 We are dedicated to ensuring that personal data is processed in alignment with the legal principles of data protection.

6.2 We implement a strategy focused on "Data Protection by Design and Default".

6.3 We can prove our adherence to data protection legislation.

6.4 Data subjects are well informed about how and why we use their data, and they can exercise their rights regarding their data.

6.5 We share personal data only when it is fair and lawful, ensuring that any data sharing is conducted securely.

6.6 We handle and report all personal data breaches, including minor ones, effectively to mitigate any potential risks and to improve our practices.

7 Data protection principles

7.1 Anyone **processing personal data** must comply with the data protection principles. We will comply with these principles in relation to any processing of personal data by the Trust. These provide that **personal data** must be:

7.1.1 **Processed** fairly and lawfully and transparently in relation to the **data subject**. This means that we only use personal data with respect for the individual who it relates to, in line with the legal grounds for processing, and we inform data subjects on how their personal data is processed including, among other ways, in our privacy notices;

7.1.2 **Processed** for specified purposes and in a way which is not incompatible with those purposes. This means that if we collect personal data for one purpose and then we need to use it for another reason, we will ensure that the new purpose is compatible with the original reason for processing;

7.1.3 Adequate, relevant and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required;

7.1.4 Accurate and up to date. This means that we will try to ensure that personal data is accurate when we collect it and kept up to date over time;

7.1.5 Not kept for any longer than is necessary for the purpose. This means that we will try to ensure that personal data is accurate when we collect it, and kept up to date over time; and

7.1.6 **Processed** securely using appropriate technical and organisational measures. Our measures include: technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and encryption, as well as organisational safeguards, including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

7.2 **Personal Data** must also:

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

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

8 Legal grounds for processing

8.1 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:

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

8.1.2 where the **processing** is necessary to comply with a legal obligation that we are subject to;

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

8.1.4 where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the **processing** prejudices the interests or fundamental rights and freedoms of **data subjects**; and

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

8.2 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:

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

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

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

8.2.4 where none of the above apply then we will seek the explicit consent of the **data subject** to the **processing** of their **special category personal data**.

8.3 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.

8.4 If any **data user** is in doubt as to the legal ground for processing **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

8.5 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 able 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

8.6 Where none of the other bases for **processing** set out above apply then the Trust must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

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

8.8 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.

8.9 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.

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

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

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

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

8.11 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. We will ensure that it will be as easy for the data subject to withdraw their consent as it was to give it.

8.12 Consent may need to be refreshed where we may need to process the **personal data** for a different and incompatible purpose which was not disclosed when the consent was first considered by the **data subject**.

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

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

9 Data subjects' rights

9.1 In addition to the right to be informed and the right to withdraw consent, we will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

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

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

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

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

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

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

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

The Right of Access to Personal Data

9.2 **Data subjects** may request access to all **personal data** we hold about them and which we are able to provide based on a reasonable and proportionate search for that personal data. Such requests will be considered in line with the schools Subject Access Request Procedure below:

9.2.1 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.

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

9.2.3 Processing SARs is free of charge, however if a request is manifestly unfounded or excessive e.g. repetitive then a reasonable fee maybe charged.

9.2.4 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.

9.2.5 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.

9.2.6 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 Trust may extend the deadline for providing the information in accordance with the provisions set out in data protection legislation.

10 Data protection by design and default

10.1 The Trust will consider and comply with the requirements of data protection legislation in relation to all its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default. In certain circumstances, where the law requires us to, we shall carry out detailed assessments of proposed processing in a Data Protection Impact Assessment (DPIA). 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 there is a change in our existing ways of working.

10.2 The Trust will complete a DPIA of any such proposed processing, and has a template document which ensures that all relevant matters are considered.

11 Data security

11.1 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**.

11.2 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.

11.3 Security procedures include:

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

11.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential.)

11.3.3 **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.

11.3.4 **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.

11.3.5 **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.

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

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

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

12 Personal data breaches

12.1 The Trust recognises that a breach of personal data could happen, despite our policies, procedures and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or personal harm to individuals.

12.2 The Trust has a personal data breach procedure, and this must be followed in relation to any actual or suspected breach of personal data.

13 Disclosure and sharing of personal information

13.1 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, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

13.2 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.

13.3 Where necessary, we will enter into a data sharing agreement to help facilitate the safe sharing of personal data.

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

14 Data Processors

14.1 We contract with various organisations who provide services to the Trust or Academy. These include people, companies, and systems that process personal data on our behalf and under our instruction.

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

14.3 **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.

14.4 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**.

15 Images and Videos

15.1 Parents and others attending Trust & Academy/School events are allowed to take photographs and videos of those events for personal and 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.

15.2 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.

15.3 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.

15.4 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.

15.5 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. Images and videos of pupils may be required for safeguarding, assessment and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust 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.

15.6 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.

16 **Video Surveillance**

CCTV footage must be handled in line with the Data Protection Principles.

Please refer to the NET Academies Trust CCTV Policy for further information.

17 **Related Policies and Documents**

CCTV Policy, Data Breach Procedure, retention schedule and Records Management Policy.

18 **Changes to this policy**

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

19 **Complaints**

19.1 Data subjects have the right to make a complaint to the Trust & Academy/School if they consider we have not complied with data protection legislation. Any complaints relating to data protection must be directed to our DPO.

19.2 When dealing with complaints relating to data protection, we shall:

19.2.1 Acknowledge receipt of the complaint within 30 days of the date on which the complaint is received by the Trust;

19.2.2 Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate;

19.2.3 Inform the complainant about progress of the complaint; and

19.2.4 Inform the complainant of the outcome of the complaint.

20 **Approval and Review**

This policy has been approved by the Board in July 2026.

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: July 2028.

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
Data protection legislation	Means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR and the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) (as amended by the Data (Use and Access) Act 2025; and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended, and all other legislation and regulatory requirements in force from time to time which apply to the use of personal data.
Data protection impact assessment (DPIA)	A tool to help identify how to comply with data protection obligations and protect individuals' rights as set out in Article 35 of the UK GDPR. The ICO also has guidance on DPIAs on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/.
Information Commissioner's Office (ICO)	In the UK, the Information Commissioner's Office (ICO) is the data protection regulator. The website of the ICO is at www.ico.org.uk.

Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Privacy notices	Where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as data controller and those of the DPO, the purpose, or purposes, and legal basis for which we intend to process that personal data, the types of third parties, if any, with which we will share, or to which we will disclose that personal data, whether the personal data will be transferred outside the UK and if so, the safeguards in place, the period for which their personal data will be stored, by reference to our [data retention policy], the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making, and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
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, if 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 Headteacher who will notify the Trust's Operations Office 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 Operations Officer 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 Operations Officer 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:	