Endeavour
Multi-Academy Trust

Data Protection Policy

Endeavour Multi Academy Trust

DOCUMENT CONTROL	
Approved for operation within	Endeavour Multi Academy Trust
Version number	V2.0
Consulted on with recognised trade unions	N/A
Reviewed by	Trust Audit & Risk Committee
Recommended to Full Trust Board by	n/a
Date approved by the Trust Board	n/a
Risk Register Item Number	N/A
Review Period	Two years
Next Review Date	Summer 2028
Policy status	Non-statutory
Location published	External
Owner	Executive Board
Author	EM/DPO Tony Dooley

DOCUMENT HISTORY DATE	DOCUMENT VERSION	DOCUMENT HISTORY
03/07/2024	V1.0	New Policy Drafting
11/06/2026	V2.0	Scheduled Review

Contents

1	Aims	4
2	Legislation and Guidance	4
3	Definitions	4
4	The Data Controller	5
5	Roles and Responsibilities	5
6	Data Protection Principles	6
7	Collecting Personal Data	7
8	Sharing Personal Data	7
9	Subject Access Requests and other rights of individuals	8
10	Parental Requests to see the Educational Records in our Schools	10
11	CCTV	10
12	Photographs and Videos in our Trust and Schools	10
13	Data Protection by Design and Default	11
14	Artificial Intelligence (AI)	11
15	Data Security and Storage of Records	11
16	Disposal of Records	12
17	Personal Data Breaches	12
18	Training	12
19	Monitoring Arrangements	12
20	Links with Other Policies	13
21	GDPR in the Trust/Schools	13
	Appendix 1: Personal Data Breach Procedure Appendix 2: Brief Information for Staff Appendix 3 – Guidance for Schools	14 17 18

1. Aims

Endeavour Multi Academy Trust ('the Trust') aims to ensure that all personal data collected about staff, pupils, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Trust and its schools process personal data relating to parents, pupils, staff, trustees, governors, visitors and others, and therefore is a Data Controller.

The Trust is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required. All schools within the Trust are included in the registration.

5. Roles and Responsibilities

This policy applies to **all staff** employed by Endeavour Multi Academy 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 Board of Trustees

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

5.2 Data Protection Officer

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 Trust data protection issues.

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

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

Our DPO for the Trust and our schools is Anthony Dooley and is contactable via Endeavour Multi Academy Trust, Tinacre Hill, Compton, Wolverhampton, WV6 8DA. Telephone 01902 761889 or email t.dooley@endeavourmat.co.uk

5.3 Data Controller

The school or the Multi Academy Trust is the Data Controller.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the Trust/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 to a third-party country or territory.
    - 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 GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

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

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

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden).
- The individual has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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

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.

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 Staffordshire County Council's Record Retention Policy.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so 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. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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, and information necessary to keep them safe while working with us.

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

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

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 to a country or territory, 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 Trust 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.
- 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.

Requests to the DPO can be made verbally, in writing, or via social media.

They should include:

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

If staff receive a subject access request, they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification.
- May contact the individual via phone to confirm the request was made.
- **Will respond without delay and within one month of receipt of the request.**
- Will provide the information free of charge.
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the individual or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other Data Protection rights of the individual

In addition to the right to make a Subject Access Request (see above), and to receive information when we are collecting their data about how we use and process it (see Section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.

- Request a copy of agreements under which their personal data is transferred to a third-party country or territory in accordance with UK Data Protection law.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the Educational Records in our schools

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.

11. CCTV

We use CCTV in various locations around the school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

Any enquiries about the CCTV system should be directed to Anthony Dooley, DPO.

12. Photographs and Videos in our Trust and Schools

As part of our Trust/school activities, we may take or use photographs and record images of individuals within our schools.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within Trust/school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on 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.

See the Mobile Phone, Camera and Image Policy and Procedures for schools for more information on our use of photographs and videos.

13. 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 privacy impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on Data Protection Law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust/school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

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 Microsoft Copilot. Endeavour 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, [school/trust name] will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

15. 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 desks, on staffroom tables, pinned to notice/display boards, 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 Trust/school office.
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment.
- 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.

16. 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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with Data Protection Law.

17. Personal Data Breaches

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

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

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a Trust context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person.
- The theft of a Trust/school laptop containing non-encrypted personal data.

18. Training

All staff, trustees and governors are provided with Data Protection training as part of their induction process.

Data Protection will also form part of Continuing Professional Development, where changes to legislation, guidance or the Trust's processes make it necessary.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated, if necessary, **every 2 years** and shared with the Board of Trustees.

20. Links with other policies

This Data Protection Policy is linked to our:

- Freedom of Information Publication Scheme.
- ICT Security Policies.
- Mobile Phone Camera and Image Policy and Procedures.
- Privacy Notices.
- Safeguarding Policies.

21. GDPR In the Trust/Schools

Endeavour Multi Academy Trust and all schools within the Trust, use the GDPR in Schools Data Management Programme. The programme stores all information about Trust and school suppliers and how they store data that the Trust/school share. The programme is used by key staff in the Trust/school to record data breaches and subject requests. Internal audits of Trust/school practice around data protection are also recorded on the programme.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Chair of Trustees/Chair of Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a protected file on the school server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concened.

        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - 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 notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on a protected file on the school server.
- The DPO and Chair of Trustees/Chair of Governors will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

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

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 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 ICT Department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive 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.

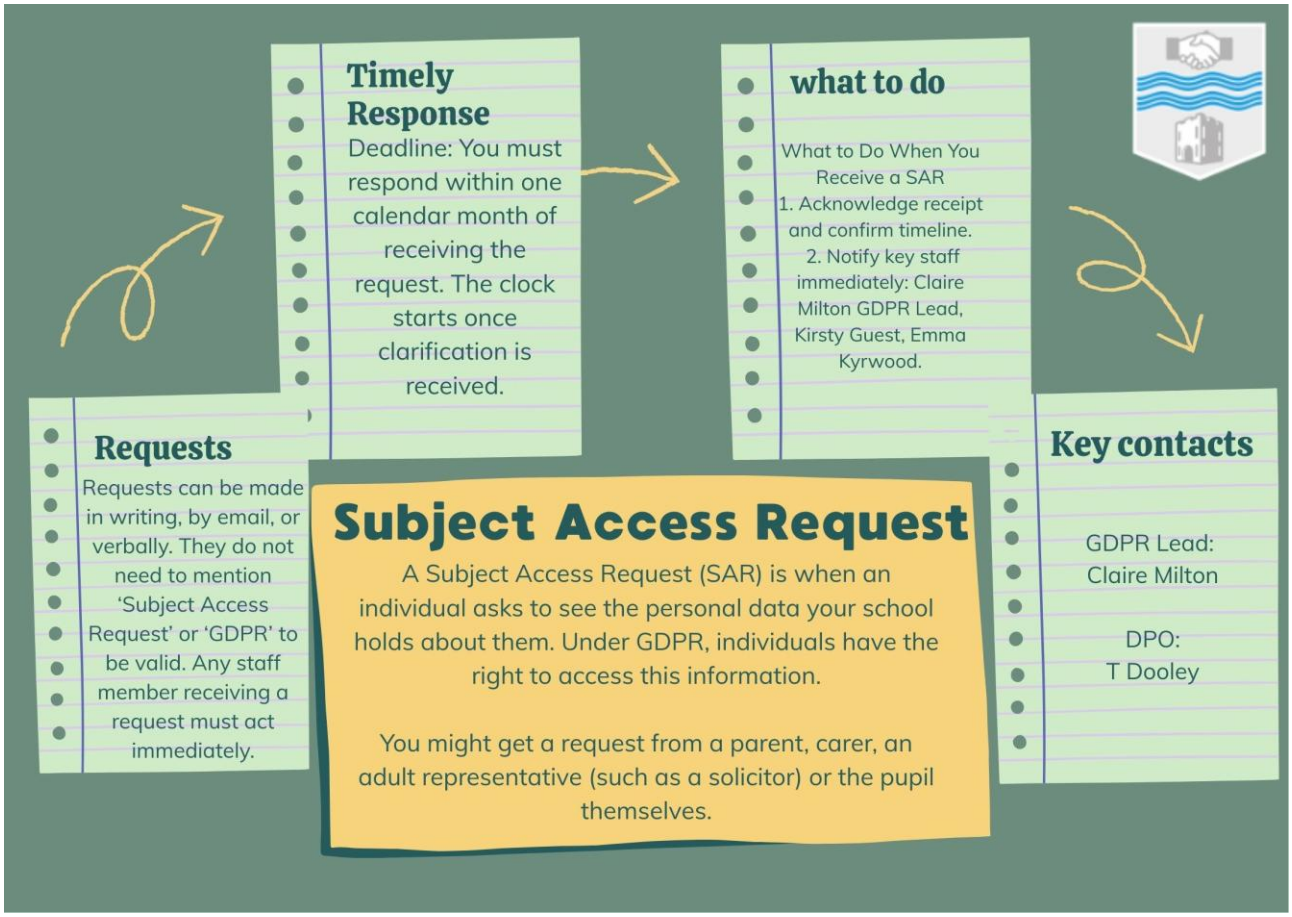
Sensitive Information Published on the Trust/school Website:

- Any examples of sensitive information being published on the Trust/schools' websites will be reported to the DPO who will record the breach.
- The Trust/school will seek to limit the number of people who have permission to publish information on the websites.
- Any breach will be reported to those affected.
- Any sensitive information will be removed as quickly as possible.

Sensitive information subject to hacking:

- All Trust/school laptops and pen sticks will be encrypted.
- Any cases of programmes, for example cashless payment systems or MIS systems, used by the Trust/school for storing sensitive information which have been hacked will be reported to the DPO and to the ICO.

APPENDIX 2 – Brief Information for Staff



APPENIDX 3 – Guidance for Schools

Subject Access Request (SAR) Guidance for Schools

This guidance outlines the procedures and responsibilities for handling Subject Access Requests (SARs) in schools, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Purpose

To ensure that all SARs are identified, processed, and responded to lawfully, fairly, and transparently, protecting the rights of individuals and maintaining compliance with data protection legislation.

2. Scope

This guidance applies to all staff, governors, and volunteers who may receive or process SARs within the school.

3. What is a Subject Access Request?

A SAR is a request made by an individual to access personal data that the school holds about them. Requests can be made verbally, in writing, or via social media.

4. Procedures for Handling SARs

a. Recognising a SAR: All staff must be trained to identify SARs.

b. Logging the Request: Record the date of receipt and details of the request.(The Trust use the GDPRiS platform for this purpose)

c. Verifying Identity: Confirm the identity of the requester before processing.

d. Clarifying Scope: Seek clarification if the request is broad or unclear.

e. Searching Records: Locate all relevant personal data.

f. Redacting Third-Party Data: Remove or anonymise data about other individuals unless consent is given or disclosure is reasonable.

g. Responding: Provide the data within one month, extendable by two months for complex requests.

h. Inform the DPO (see information re the GDPRiS platform above.

5. What Must Not Be Included in SARs

- Third-party personal data without consent or justification.
- Confidential references.
- Information that could cause serious harm to any individual.
- Legally privileged information.
- Exam scripts and certain educational records.
- Data about deceased individuals.

6. Special Cases

- Requests involving children: Assess the child’s competence to make the request.
- Requests during holidays: Must still be processed within the legal timeframe.
- Requests from third parties: Require evidence of authority to act on behalf of the individual.

7. Enforcement and Compliance

- Failure to comply may result in ICO enforcement actions, fines, or legal claims.
- It is a criminal offence to destroy or conceal data to avoid disclosure.

8. Review of Guidance

This guidance will be reviewed annually or in response to changes in legislation or guidance.

Subject Access Requests – Further Information

1. Understanding the Right of Access

- Individuals have the right to:
  - Confirmation of data processing.
  - Access to their personal data.
  - Supplementary information (e.g., processing purposes, data categories, recipients, retention periods).

2. Recognising Subject Access Requests (SARs)

- No formal wording required; can be made verbally, in writing, or via social media.
- Organisations must train staff to identify and handle SARs appropriately.

3. Responding to SARs

- Must respond within one month, extendable by two months for complex requests.
- May request ID or clarification if necessary.
- Must provide data in a commonly used format and ensure secure delivery.

4. Refusing a Request

- Can refuse if the request is:
  - **Manifestly unfounded** (e.g., malicious intent).
  - **Manifestly excessive** (e.g., disproportionate burden).
- Exemptions apply in specific contexts (e.g., legal privilege, crime prevention, journalism).

5. Third-Party Data

- Must balance the requester's rights with third-party privacy.
- Disclosure may be allowed with consent or if reasonable without consent.

6. Special Categories of Data

- **Health, education, and social work data** have additional rules and exemptions.
- Disclosure may be restricted if it causes serious harm or breaches confidentiality.

7. Special Cases

- Includes rules for:
  - Unstructured manual records (especially for public authorities).
  - Credit files.
  - Requests involving children or deceased individuals.

8. Enforcement and Legal Implications

- ICO can issue warnings, reprimands, or fines.
- Individuals can seek compensation or court orders.
- Criminal offences include:
  - Forcing someone to make a SAR.
  - Destroying or concealing data to avoid disclosure.

Practical Advice

- Organisations should:
  - Prepare policies and procedures for handling SARs.
  - Maintain data inventories and retention schedules.
  - Train staff and ensure secure systems for data access and delivery.

Key Points from ICO Right of Access Guidance

- Individuals have the right to access their personal data and supplementary information.
- SARs can be made in any format and do not require specific wording.
- Schools must respond within one month, extendable by two months for complex cases.
- Identity verification and clarification may be requested.
- Disclosure must be secure and in a commonly used format.
- Exemptions apply for third-party data, legal privilege, and data causing harm.
- Special rules apply for health, education, and social work data.
- ICO can enforce compliance and issue penalties.
- It is a criminal offence to force someone to make a SAR or to destroy data to avoid disclosure.

What Must Not Be Included in SARs in Schools

- Third-party personal data without consent or justification.
- Confidential references for education, employment, or volunteering.
- Information that could cause serious harm to any individual.
- Data provided under expectation of confidentiality.
- Legally privileged information.
- Information about deceased individuals.
- Exam scripts (answers written by candidates).
- Management forecasts or negotiation details.
- Unstructured manual records if retrieval cost exceeds legal threshold.

Staff Development SARs

Part 1: Introduction to SARs

Discussion Questions:

1. What is a Subject Access Request (SAR)?
2. Why is the right of access important for pupils, parents, and staff?
3. Who can make a SAR and in what formats?

Activity:

- Break into small groups and list all the ways a SAR might be received in a school setting (e.g., email, verbal request, social media).

Part 2: Recognising and Responding to SARs

Scenario Exercise: Read the following scenario and answer the questions:

A parent emails the school asking for "all the information you hold about my child." The child is 13 years old.

Questions:

1. Is this a valid SAR?
2. Who has the right to access the data?
3. What steps should the school take next?

Key Learning Points:

- SARs do not need to mention GDPR or use formal language.
- The child may be competent to make their own request.
- Identity verification and clarification may be needed.

Part 3: Handling Third-Party Data

Role Play: Staff members act out a scenario where a SAR includes information about other pupils or staff.

Debrief:

- Discuss when it is appropriate to redact or withhold third-party data.
- Explore the balance between the requesters rights and others confidentiality.

Part 4: Timeframes and Extensions

Quiz:

1. How long do you have to respond to a SAR?
2. When can you extend the deadline?
3. What is the "stop the clock" rule?

Answers:

- One month from receipt.
- Extension allowed for complex requests or multiple simultaneous requests.
- Clock stops when clarification is requested.

Part 5: Special Cases in Schools

Group Discussion:

- How should SARs be handled during school holidays?
- What are the rules for educational records vs. general personal data?

Case Study:
A parent requests their child's disciplinary record. The teacher has handwritten notes not shared with others.

Questions:
1. Is this part of the educational record?
2. Should it be disclosed?

Part 6: Practical Steps and Good Practice

Checklist Creation: Each group creates a checklist for handling SARs in their school, including:
- Logging the request
- Verifying identity
- Clarifying scope
- Searching records
- Redacting third-party data
- Responding securely
-

Wrap-Up:
- Share checklists.
- Discuss how to improve SAR handling procedures.

[Insert your school's name and address] [Insert date]

Re: subject access request

Dear [insert the name of the individual who submitted the subject access request]

Please find enclosed the information that you requested under the UK General Data Protection Regulation (UK GDPR).

Your name	[Insert requester's name]
Your relationship with the school	[Pupil / parent / carer/ employee / governor / volunteer / other (specify)]
Details of the information you requested/enclosed	[Insert details of the specific information requested, such as: › Your personnel file › Your child's medical records › Your child's behaviour record, held by [insert class teacher's name] › Emails between 'person A' and 'person B' between [date]]
Date you requested the information	[Insert date]
Date we supplied the information	[This must be within 1 month of the above date, except in the case of an extension or delay, e.g. in receiving ID]
Format we supplied the information	[For example, encrypted USB stick accompanying this letter]

If you need any further advice relating to your subject access request, you can contact:

[Insert name and method for contacting the data protection officer at your school]

Yours sincerely,

[Name]