Diocese of Norwich Education and Academies Trust

Data Protection Policy

Policy Type:	**Trust Policy**
Date Issued by MAT:	**10/09/2026**
Approved By:	**Joint Policy Development Committee**
Approval Date:	**03/09/2026**
Review Date:	**September 2027**
Person Responsible:	**Head of Governance**

Our Christian Ethos and Values

All policies within the Diocese of Norwich Education and Academies Trust (hereafter referred to as "the Trust"), whether relating to an individual academy or the whole Trust, will be written and implemented in line with our Christian ethos and values.

We have high ambition for all, and we truly value the wider educational experience.

We walk and talk our Christian values. We put people at the centre of the organisation and want to see them flourish and grow. Our schools are inclusive, welcoming those of all faiths and none.

Overall accountabilities and roles

The Trust has overall accountability for all its academies and staff. Through a Scheme of Delegation it sets out the responsibilities of the Trust, its Executive Officers, the Local Governance Committee and the Principal / Headteacher. The Principal / Headteacher of each academy is responsible for the implementation of all policies of the Trust.

All employees of the Trust are subject to the Trust's policies.

Contents

1. Aims

Our Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:
UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
Data Protection Act 2018 (DPA 2018)
The Data Use and Access Act 2025 (DUAA)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

For schools that use biometric data it meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

For schools that use CCTV it also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

The Data Protection Officer (DPO) is Hannah Monk, Head of Governance and is contactable via governance@donesc.org and 01603 550150.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Term	Definition
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 processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered with the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by the 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 The Trust board

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

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Trust board and, where relevant, report to the board their advice and recommendations on school and Trust data protection issues.

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

The DPO is Hannah Monk, Head of Governance and is contactable via governance@donesc.org and 01603 550150.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles that the Trust and all its schools must comply with.
The principles say that personal data must be:

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

This policy sets out how the school 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 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school or Trust can **fulfil a contract** with the individual, or the individual has asked the Trust or school to take specific steps before entering into a contract.
- The data needs to be processed so that the school or Trust can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, i.e. to protect someone's life.
- The data needs to be processed so that the school or Trust, as a public authority, can **perform a task in the public interest or exercise its official authority.**
- The data needs to be processed for the **legitimate interests** of the school or Trust (where the processing is not for any tasks the school or Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, we will **also** meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent.**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

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

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

7.2 Limitation, minimisation and accuracy

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

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

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

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

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

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.

- Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with government bodies where we are legally required to do so and the police when we are requested to do so.

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

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form, they may contact the Trust DPO for advice via the DoNESC Helpdesk.

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.

There is no fixed age presumption in England, Wales and Northern Ireland for a child to understand their rights. Every instance should be considered on an individual basis and the outcome of the consideration should be documented.

9.3 Responding to subject access requests.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.

- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- Will make reasonable and proportionate searches when someone asks for access to their personal information.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of any individual.
- Would reveal that a child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

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

When we refuse a request, we will tell the individual why, and tell them they have the right to complain or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual
In addition to the right to make a subject access request (see above), and to receive information when 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 (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement).
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

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

10. Parental requests to see the educational record
In academies, there is no automatic parental right of access to the educational record, but we will usually choose to provide information on request.

11. Biometric recognition systems
Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

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

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

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

13. Photographs and videos

As part of our activities, we may take photographs and record images of individuals within our schools.

We will obtain written consent from the children and/or their parents/carers for photographs and videos to be taken 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.

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

Where the school takes photographs and videos, uses may include:

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

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school, Trust 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

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 and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office and are responsible for ensuring its security while it is in their possession.
- All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords that are at least 10 characters long containing letters and numbers are recommended to access school computers, laptops and other electronic devices. Our IT providers use strength checkers to check the suitability of passwords. Staff and pupils are reminded that they should not reuse passwords from other sites. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- Staff may only use personal devices (including computers and phones) to access Trust data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher or CEO. Staff should be using Trust approved methods (given in the ICT Acceptable Use Policy) to share files. Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by OfficeXpress and staff should be using Trust approved methods for file sharing.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our ICT and Internet acceptable policy and agreements).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

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 school or 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

We will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.
When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.
Such breaches in a school context may include, but are not limited to:

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

18. Training

All staff are provided with data protection training as part of their induction process and governors are signposted to suitable training. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring and review

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by the Joint Policy Development Committee.

20. Links with other policies

This data protection policy is linked to our:
Data Protection Complaint's Procedure
Safeguarding Policy
ICT and Internet Acceptable Use Policy
Privacy Notices for Staff, Parents, Pupils and Governors and Trustees

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member, governor, trustee, volunteer or data processor must immediately notify the data protection officer (DPO) by completing the online DB9 form on the Staff area of the Trust Website.
- 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.
- Individuals will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the individual responsible and the headteacher or executive leader where the breach has occurred. Depending on the severity they may also inform members of the Trust team.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers).
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned.
        - The categories and approximate number of personal data records concerned.
        - The name and contact details of the DPO.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If not all the above details are yet known, the DPO will report as much as they can within 72 hours of the being made aware of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school or Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored.
- The DPO will review data breach records regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school or Trust to reduce risks of future breaches.

Appendix 2: Subject Access Request Procedure

Recognising a Subject Access Request
A Subject Access Request does not need to be made in a particular format – it can be verbal, or in writing, by email, on social media or on paper.

In schools we can reasonably expect that the majority of Subject Access Requests will be from parents requesting their child's data although it is worth being aware that employees, volunteers and anyone about whom the school holds personal data may also make Subject Access Requests.

On receipt of a Subject Access Request we will:

- Start a record/log of actions related to the Subject Access Request.
- Consider whether they should seek the consent of a pupil whose information has been requested. This will depend on the child's capacity to understand consent and what is being asked for so must be considered on a case-by-case basis and using the school team's professional judgement. Make a record of our consideration and decision.
- Seek to verify the identity of the person requesting the data by:
  Requesting 2 forms of ID.
  Contacting the individual by phone to confirm the request was made.
- Once confirmation has been received, the school has **one month** to supply the information.

Increasingly parents submit a Subject Access Request to a school to obtain information to inform an application for additional support for their child. If the request references such a purpose it is worth following up with the parent to ask if there is specific information they need. It may be that they do not need, and do not want, every email, document and file referencing their child so following up from a customer service angle might help everyone.

If it turns out that the parent does not require their Subject Access Request after all they will need to withdraw the request. We will follow up with them and record the outcome.

Data Assembly
The next step is to identify where data about the data subject is held. This may include but is not limited to:

- Emails
- MIS
- Safeguarding/incident reports (online or paper)
- Personnel records
- Documents in cloud storage solutions (OneDrive, SharePoint, GoogleDrive)

The school should expect to assemble data from its MIS, Safeguarding systems, personnel records, and anything else easily accessible onsite.
To retrieve emails and cloud-stored documents, we recommend that the school contacts their IT provider to conduct a search and retrieval.

Review and Redaction
All data must be reviewed to identify the data of others that needs to be redacted – see below – and for items that should be withheld due to either safeguarding or because providing the data would pose a risk of harm to either the data subject, the requester or another individual.

All information related to individuals other than the data subject, that is not available in the public domain, must be thoroughly redacted.

Providing the information
If the individual submitted the Subject Access Request electronically (e.g. by email or via social media), we will provide a copy in a commonly used electronic format. We may choose the format, unless the requester makes a reasonable request for you to provide it in another commonly used format (electronic or otherwise).

If the individual submitted the Subject Access Request by other means (e.g. by letter or verbally), we will provide a copy in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for you to provide it in another commonly used format. However, where the information is sensitive, we will ensure that we transfer it to the requester using an appropriately secure method.

The sender should follow up with the requester to confirm that the data has been received and record that the Subject Access Request has been completed.

Once completed the school or Trust team will log the request, forming part of a record managed by the DPO.

Requests by others

If a request is received "on behalf of" an individual we will check its authenticity. If a consent form is included with the request, contact the individual using contact details already held.

Other organisations requesting information about an individual, such as the police (unless warranted) or HMRC are not making Subject Access Requests and so a Legal Processing Condition will need to be identified. Do not be afraid to ask questions to satisfy either,

- Compliance with a legal obligation, or
- Legitimate Interest, or
- Recognised Legitimate Interest

More information for Trust staff is available in the staff area of the Trust website.

Appendix 3: Data Protection Impact Assessment Procedure

The Trust will undertake a Data Protection Impact Assessment (DPIA) where processing of personal data is likely to result in a high risk to the rights and freedoms of individuals or where a new process or technology is being considered. DPIAs will be completed in accordance with the UK GDPR, Data Protection Act 2018, applicable provisions of the Data (Use and Access) Act 2025, and current ICO guidance.

A DPIA will be considered at the earliest stage of any new project, system, service or process involving personal data and whenever there is a significant change to existing processing. This includes the introduction of new IT systems, EdTech, artificial intelligence, biometric technology, monitoring systems, large-scale processing, profiling, automated decision-making, significant data sharing, or processing involving children, vulnerable individuals or special category data.

Where a DPIA is required, the project owner will complete the Trust's DPIA template with support from the DPO and relevant technical, safeguarding, HR, procurement or other specialists.

The assessment will document the nature, scope, context and purposes of processing and assess whether the processing is necessary and proportionate. It will identify potential risks to individuals, considering both the likelihood and severity of harm. Particular consideration will be given to children's rights and expectations, special category data, confidentiality, discrimination, security risks and the potential for physical, financial or other significant harm.

The DPIA will identify measures to eliminate, reduce or manage identified risks. These may include data minimisation, access restrictions, encryption, pseudonymisation, retention controls, contractual safeguards, transparency measures and human oversight.

The DPO will be consulted during the DPIA process and will provide advice on compliance and risk mitigation. Relevant stakeholders, including staff, IT providers, and suppliers, will be consulted where appropriate.

The project owner will ensure that identified mitigation measures are implemented before processing begins. The DPO will approve the DPIA, taking account of any residual risks.

Where high residual risks remain that cannot be sufficiently mitigated, the Trust, usually through the DPO, will consult the ICO before commencing the processing where legally required.

A DPIA is a living document and will not be treated as a one-off exercise. The project owner will ensure that the processing continues to operate in accordance with the approved DPIA and that identified controls remain effective.

The DPIA will be reviewed periodically and whenever there is a significant change to the nature, scope, purpose or technology involved, or where a new risk is identified. DPIAs will be retained as evidence of the Trust's accountability and made available to the DPO, auditors or ICO where appropriate.

No high-risk processing covered by this process should commence until the required DPIA has been completed, approved and any necessary risk mitigation measures implemented

Appendix 4: Retention of Personal Data

How long you keep different types of data will depend on whether you're keeping it for operational needs or to comply with legal requirements.

The following records have statutory retention periods. You should decide how long you need to keep other records, in line with the business need of the school or Trust.

Source: https://www.gov.uk/guidance/data-protection-in-schools/record-keeping-and-management

Pupil records

Document type	Retention period	Action at end of retention period	Further information
Primary school pupil records	Until the pupil leaves the school.	Transfer to secondary school or other primary school when the pupil leaves.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the pupil record. There is guidance on how to transfer information to another school.
Secondary school pupil records	Until the pupil's 25th birthday.	Dispose of records securely. If the pupil leaves to go to another school, transfer the records to that school. There is guidance on what to do if the school closes before the end of the retention period.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the education record. Retain as detailed in section 2 of the Limitation Act 1980.
Special educational needs and disabilities (SEND), including SEND statements and accessibility plans	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.
Attendance and absence	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980.

Child protection records

Document type	Retention period	Action at end of retention period	Further information
Child protection files	Until the child's 25th birthday. If the file relates to child sexual abuse, retain until the child's 75th birthday.	Dispose of records securely. Child protection files should be passed on to any new school a child attends. This should be transferred separately from the main pupil file.	Should be stored in a separate child protection file. Keeping children safe in education sections 66, 67, 121 and 122. The Report of the Independent Inquiry into Child Sexual Abuse (IICSA), recommendation on access to records.
Allegations of child protection against a member of staff, including unfounded allegations	Until the staff member's normal retirement age, or 10 years from the date of the allegation, whichever is later.	Dispose of records securely.	Keeping children safe in education. Working together to safeguard children.

Finance records

Document type	Retention period	Action at end of retention period	Further information
Contracts	6 years from the last payment on the contract.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Debtor's records	6 years from the end of the financial year.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
VAT records	6 years from the end of the financial year.	Dispose of records securely.	May include invoices, budgets, bank statements and annual accounts. Record keeping (VAT Notice 700/21).

Governance records

Document type	Retention period	Action at end of retention period	Further information
Admissions	6 years from the admission date.	Dispose of records securely.	Working together to improve school attendance.

Document type	Retention period	Action at end of retention period	Further information
Attendance registers	3 years from the date of entry.	Dispose of records securely.	Regulation 14 of the Education (Pupil Registration) (England) Regulations 2006.
Curricular record	At least one year.	Dispose of records securely.	The Education (School Records) Regulations 1989. Regulation 3 of the Education (Pupil Information) (England) Regulations 2005.
Directors – disqualification	15 years from the date of disqualification.	Dispose of records securely.	The Education (Company Directors Disqualification Act 1986: Amendments to Disqualification Provisions) (England) Regulations 2004
Records of educational visits	10 years from the date of the visit, if there was an incident on the visit, retain the permission slips for all pupils and the incident report in the pupil record, or until the pupil reaches the age of 25.	Dispose of records securely.	Health and safety on educational visits. Retain as detailed in section 2 of the Limitation Act 1980.
School vehicles	6 years from the disposal of the vehicle.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Statutory registers and compliance	Retention periods vary, for example: Memorandums of understanding should be retained for the life of the academy plus 6 years. Annual reports should be retained for 10 years from the date of the report. Board meeting records should be retained for 10 years from the date of the meeting.	Dispose of records securely.	May include annual reports and governance records. Companies Act 2006 contains information on which statutory registers to keep. Compliance guidance in the maintained schools governance guide. Compliance guidance in

Document type	Retention period	Action at end of retention period	Further information
			the academy trust governance guide. Academy trust handbook.

Health and safety records

Document type	Retention period	Action at end of retention period	Further information
Accessibility plans	Life of plan plus 6 years.	Dispose of records securely.	Retain as detailed in section 2 of the Limitation Act 1980.
Accident records	3 years from the date of the accident.	Dispose of records securely.	Accidents involving pupils should be retained in the pupil record. Regulation 25 of the Social Security (Claims and Payments) Regulations 1979.
Monitoring exposure to substances hazardous to health, including asbestos	5 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002.
Health surveillance records	40 years.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Other health records of staff	While the worker is employed in your school.	Dispose of records securely.	The Control of Substances Hazardous to Health Regulations 2002. Health surveillance - Record keeping.
Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	Fire Service Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.

Property records

Document type	Retention period	Action at end of retention period	Further information
Maintenance records	6 years from the end of the financial year.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	12 years from the end of the deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980.

Staff records

Document type	Retention period	Action at end of retention period	Further information
Copies of DBS certificates	6 months from the date of recruitment.	Dispose of records securely.	Keeping children safe in education.
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends.	Dispose of records securely.	The Statutory Maternity Pay (General) Regulations 1986.
Pay records	3 years from the end of the tax year they relate to.	Dispose of records securely.	PAYE and payroll for employers: Keeping records.
Personnel files	6 years from termination of employment.	Dispose of records securely.	Section 2 of the Limitation Act 1980.
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed.	Dispose of records securely.	Regulation 15 of the Retirement Benefits Schemes (Information Powers) Regulations 1995.