DIOCESE OF

ST ALBANS

MULTI-ACADEMY TRUST

Trust Policy

Data Protection

Policy type	**Trust Policy (Tier 1)**
Reviewed	**Every 3 years**
Author/Responsible Officer	**Data Protection Officer**
Board to be ratified	**Audit and Risk Committee**
Approved by	**Trust Board**
Date of ratification	**May 2025**
Date of next review	**May 2028**

This policy is a mandatory policy for all DSAMAT staff and must be implemented without any amendments

Enabling all to flourish: Rooted in God's love

Our mission, vision and values

The Trust has a clear mission at its core, ensuring that all pupils are enabled to flourish, rooted in God's Love - academically, socially, spiritually, physically and mentally. This is central to our work and rooted in our Christian foundation (John 10 v 10). Our commitment to mutual flourishing within the school community is built upon our shared belief in Church of England principles. In our Trust, just as in the wider Church of England community, 'flourish' refers to prospering, thriving and growing – not shrinking out and dying. It means prayerfully encouraging all within our schools so that they might prove fruitful, successful and contented in the longer term. We seek to provide space generously for all to flourish in life and all of its structures. Equal treatment for all pupils, staff and the wider community is a core part of enabling this long term, holistic flourishing.

We have a clear vision about creating successful schools for the benefit of their communities. All schools provide rich and diverse curricula which evolve to meet the needs of their children and local communities, as well as delivering educational excellence to enable them to continue to flourish in later life.

The way we work and deliver against our mission is critical to our Trust. We have shared, agreed values of:

Hope; Nurture; Equality; Respect; Collaboration

The Trust's vision is underpinned by a Christian values framework which is adopted by all schools. It provides clear expectations for all Trust employees on how we wish our values to impact on all areas of school life. It draws on, and is informed by, the National Church of England Vision for Education and the Diocesan Board of Education Vision.
Each school within the Trust has a personalised vision for education, developed locally to reflect the individual character and needs of the school community. This vision is underpinned by the Trust's wider vision, and agreed with the Trust, but it is owned and driven by the headteacher and their LGB.

Our community

The Trust are dedicated to delivering education that serves local communities. Our schools are inclusive, welcoming those from all and no faiths, from all abilities and backgrounds. We believe in providing a high-quality education, underpinned by Christian values, which enables every child to flourish.

Underpinning all of the Trust's work is a belief in educational excellence. The Trust serves all stakeholders by providing schools with the highest levels of academic rigour and pastoral care.
Our schools are places where children and young people develop and thrive intellectually, socially, culturally and spiritually. All of the Trust's schools teach a broad and balanced curriculum within national guidelines focusing on core skills. This is designed to ensure that all pupils reach their academic potential and seek to enrich their experience along the way. Pupils will be enabled to succeed in an atmosphere of high expectation, aspiring to educational excellence with a firm foundation of values.

This policy forms part of our Trust governance and ensures that we are held to the highest standards as we carry out our duties.

Contents:

Statement of intent

This is the Diocese of St Albans Multi-Academy Trust (DSAMAT) over-arching Data Protection Policy and must be implemented and adhered to in each of the academies within the Diocese of St Albans Academy Trust along with those working within the central team.

This policy will also be implemented and adhered to from the first day of any other academy joining the Trust.

For the remainder of this document, the Diocese of St Albans Multi Academy Trust will be referred to as DSAMAT.

Schools within the Diocese of St Albans Multi Academy Trust are required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under data protection legislation.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the UK GDPR and understands the threats faced and how to protect the information held.

Organisational methods for keeping data secure are imperative, and the school believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UKGDPR) 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Data Protection Act 2018 (DPA)
- Electric Commerce (EC Directive) Regulations 2003
- Protection of Freedoms Act 2012
- Current version of DfE 'Keeping Children Safe in Education'

This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO(2012)'IT asset disposal for organisations
- DfE(2023)'Data protection: a toolkit for schools'

This policy will be implemented in conjunction with the following other school policies and procedures:

- IT Acceptable Use Policy
- Cyber Security Policy
- Protection of Biometric Information Policy (where applicable)
- Freedom of Information Policy and Model Publication Scheme
- Surveillance and CCTV Policy (where applicable)
- Child Protection and Safeguarding Policy
- Records Management Policy

2. Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation

Personal data which reveals:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.

'**Sensitive personal data'** does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

3. Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

4. Accountability

DSAMAT and its Academies will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

DSAMAT will provide comprehensive, clear and transparent privacy policies.
Additional internal records of the trust and school's processing activities will be maintained and kept up to date.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.
- Internal records of processing activities will include the following:
- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

DSAMAT and its Academies will also document other aspects of compliance with the UK GDPR and Data Protection Act where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches
- A log of access to CCTV footage, including the reason for access, who authorised it, and when it occurred. Requests should be recorded using a standard form (example at the end of this policy) and stored securely either in hard copy or digitally.
- The school will implement measures that meet the principles of data protection by design and data protection by default, such as:
- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.

- Continuously creating and improving security features.
- DPIAs will be used to identify and reduce data protection risks, where appropriate.

5. Data protection officer (DPO)

The DPO is appointed as Handsam Ltd and will:

- Inform and advise the Trust and its employees and volunteers about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor DSAMAT and its Academies' compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.
- Report to the highest level of management at the Trust, which is the Chair of the Board of Directors, through the Head of Estates.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on riskier activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.

6. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

DSAMAT and its Academies will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law.

When none of the above apply, consent will be obtained by the data subject to the processing if their special category personal data.

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

- That the personal data is being processed
- Why the personal data is being processed
- What the lawful basis is for that processing
- Whether the personal data will be shared, and if so, with whom
- The existence of the data subject's rights in relation to the processing of that personal data
- The right of the data subject to raise a complaint with the ICO in relation to any processing

DSAMAT has privacy notices for the following groups, which outline the information above that is specific to them:

- Prospective employees
- Pupils and their families
- School workforce
- Third parties
- Directors and governors

- Volunteers

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 may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where DSAMAT and its Academies relies on:

- 'Performance of contract' to process a child's data, the school / Trust considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school / Trust takes responsibility for identifying the risks and consequences of the processing and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school / Trust ensures that the requirements outlined in on page 15 are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

7. Consent

- Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.
- DSAMAT and its Academies ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- Where the school / Trust opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.
- In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school / Trust on a case-by-case basis, taking into account the requirements outlined in section 7.

8. Right to be informed

- Adults and children have the same right to be informed about how DSAMAT and its Academies uses their data.

- The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language, which is concise, transparent, easily accessible and free of charge.
- In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:
- The identity and contact details of the controller, the controller's representative, where applicable, and the DPO.
- The purpose of, and the lawful basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
- Withdraw consent at any time.
- Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
- Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
- For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

- Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed.
- Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.
- The school will verify the identity of the person making the request before any information is supplied.

- A copy of the information will be supplied to the individual free of charge; however, the school / Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, the school / Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:
- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received.

10. The right to rectification

- Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.
- Where the personal data in question has been disclosed to third parties, the school / Trust will inform them of the rectification where possible.
- Where appropriate, the school / Trust will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

- DSAMAT and its Academies will take reasonable steps to ensure that data is accurate or are rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data.
- DSAMAT and its Academies will restrict processing of the data in question whilst its accuracy is being verified, where possible.
- The school / Trust reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.
- Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school / Trust will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

- Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Individuals, including children, have the right to erasure in the following circumstances:
    - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
    - When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - The personal data was unlawfully processed
    - The personal data is required to be erased in order to comply with a legal obligation
    - The personal data is processed in relation to the offer of information society services to a child
- The school / Trust will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.
- The school / Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
    - For public health purposes in the public interest
    - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
    - The establishment, exercise or defense of legal claims
- The school / Trust has the right to refuse a request for erasure for special category data where processing is necessary for:
    - Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.

    - Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.
- Requests for erasure will be handled free of charge; however, the school / Trust may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.
- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, the school / Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

- Individuals, including children, have the right to block or suppress DSAMAT and its Academies processing of personal data.
- In the event that processing is restricted, the school / Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- DSAMAT and its Academies will restrict the processing of personal data in the following circumstances:
    - Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
    - Where an individual has objected to the processing and the school / Trust is considering whether their legitimate grounds override those of the individual
    - Where processing is unlawful, and the individual opposes erasure and requests restriction instead
    - Where the school / Trust no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim
- If the personal data in question has been disclosed to third parties, the school / Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where DSAMAT and its Academies are restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.
- The school / Trust will inform individuals when a restriction on processing has been lifted.
- DSAMAT and its Academies reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their

right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

13. The right to data portability

- Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.
- Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
- The right to data portability only applies in the following cases:
  - Where personal data has been provided directly by an individual to a controller
  - Where the processing is based on the individual's consent or for the performance of a contract
  - When processing is carried out by automated means
- Personal data will be provided in a structured, commonly used and machine-readable form.
- The school / Trust will provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- DSAMAT and its Academies are not required to adopt or maintain processing systems which are technically compatible with other organisations.
- In the event that the personal data concerns more than one individual, the school / Trust will consider whether providing the information would prejudice the rights of any other individual.
- DSAMAT and its Academies will respond to any requests for portability within one month.
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- Where no action is being taken in response to a request, the school / Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. The right to object

- DSAMAT and its Academies will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
- Individuals, including children, have the right to object to the following:
  - Processing based on legitimate interests or the performance of a task in the public interest
  - Processing used for direct marketing purposes
  - Processing for purposes of scientific or historical research and statistics.

- Where personal data is processed for the performance of a legal task or legitimate interests:
  - An individual's grounds for objecting must relate to his or her particular situation.
- The school / Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defense of legal claims, or, where the school / Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- DSAMAT and its Academies will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.
- Where personal data is processed for direct marketing purposes:
  - The right to object is absolute and the school / Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
  - DSAMAT and its Academies cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
  - The school / Trust will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.
- Where personal data is processed for research purposes the individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school / Trust is not required to comply with an objection to the processing of the data.
- The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings.
- Where the processing activity is outlined above, but is carried out online, the school / Trust will offer a method for individuals to object online.
- DSAMAT and its Academies will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.
- Where no action is being taken in response to an objection, the school / Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.
- The DSAMAT Complaints Policy is available to use in the case of dissatisfaction.

15. Automated decision making and profiling

- DSAMAT and its Academies will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:
  - Necessary for entering into or performance of a contract.
  - Authorised by law.
  - Based on the individual's explicit consent.
- Automated decisions will not concern a child nor use special category personal data, unless:

  - The school has the explicit consent of the individual.
  - The processing is necessary for reasons of substantial public interest.
- The school / Trust will conduct a data protection impact assessment (DPIA) for automated decision making to mitigate risk of errors, bias and discrimination.
- The school / Trust will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.
- Individuals have the right not to be subject to a decision when both of the following conditions are met:
  - It is based on automated processing, e.g. profiling
  - It produces a legal effect or a similarly significant effect on the individual
- DSAMAT and its Academies will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.
- When automatically processing personal data for profiling purposes, the school / Trust will ensure that the appropriate safeguards are in place, including:
  - Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
  - Using appropriate mathematical or statistical procedures.
  - Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
  - Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16. Data protection by design and default

- DSAMAT and its Academies will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into all aspects of processing activities.
- In line with the data protection by default approach, DSAMAT and its Academies will ensure that only data that is necessary to achieve its specific purpose will be processed.
- DSAMAT and its Academies will implement a data protection by design and default approach by using a number of methods, including, but not limited to:
  - Considering data protection issues as part of the design and implementation of systems, services and practices.
  - Making data protection an essential component of the core functionality of processing systems and services.
  - Automatically protecting personal data in school ICT systems.
  - Promoting the identity of the DPO as a point of contact.
  - Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

17. Data Protection Impact Assessments (DPIAs)

- DPIAs will be used in certain circumstances to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.
- DPIAs will allow the school / Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school / Trust reputation which might otherwise occur.
- A DPIA must be produced in advance of any change of data processing activity or before the installation of any new software of any kind and this must be reviewed and approved by Partnership Education and / or Handsam.
- A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- A DPIA will be used for more than one project, where necessary.
- High risk processing includes, but is not limited to, the following:
  - Systematic and extensive processing activities, such as profiling
  - Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
  - The use of CCTV.
- The school will ensure that all DPIAs include the following information:
  - A description of the processing operations and the purposes
  - An assessment of the necessity and proportionality of the processing in relation to the purpose
  - An outline of the risks to individuals
  - The measures implemented in order to address risk
- Where a DPIA indicates high risk data processing, the school / Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

18. Data breaches

- The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- The headteacher/ line manager will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their training.
- Where the school / Trust faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
- In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school / Trust will notify those concerned directly.
- A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

- In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- Effective and robust breach detection, investigation and internal reporting procedures are in place at DSAMAT and its Academies, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
- Within a breach notification to the supervisory authority, the following information will be outlined:
  - The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
  - The name and contact details of the DPO
  - An explanation of the likely consequences of the personal data breach
  - A description of the proposed measures to be taken to deal with the personal data breach
  - Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- Where notifying an individual about a breach to their personal data, the school / Trust will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.
- The school / Trust will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.
- The school / Trust will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

19. Data security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Whilst the school/Trust does not provide personal devices for all employees and volunteers, they are expected to abide by the IT acceptable Use Policy and the Data

Retention Schedule to ensure any documents that are downloaded are secure and erased within the appropriate timeframe.

- All necessary employees and volunteers are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
  - They are allowed to share it.
  - That adequate security is in place to protect it.
  - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school / Trust containing sensitive information are supervised at all times.
- The physical security of the DSAMAT and Academies buildings and storage systems, and access to them, is reviewed on a termly bases. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- The school / Trust will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.
- DSAMAT and its Academies takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The headteacher / line manager is responsible for continuity and recovery measures are in place to ensure the security of protected data. They may delegate this responsibility to another member of staff.
- When disposing of data, paper documents will be shredded, and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets Retention and destruction of information | ICO.
- The school / Trust holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

20. Safeguarding

- DSAMAT and its Academies understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.
- DSAMAT and its Academies will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing

information must not be allowed to obstruct the need to safeguard and protect pupils. The headteacher / line manager will ensure that staff are:

  - Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
  - Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.
- The school / Trust will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible.
- Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:
  - Whether data was shared
  - What data was shared
  - With whom data was shared
  - For what reason data was shared
  - Where a decision has been made not to seek consent from the data subject or their parent
  - The reason that consent has not been sought, where appropriate
- The school / Trust will aim to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk.
- DSAMAT and its Academies will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.
- Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the school / Trust will see independent legal advice
- All data breaches, including near misses, must be recorded using the Handsam online Breach Log, which provides a secure platform for logging incidents and enables appropriate members of the Trust's central team to review and respond. Where necessary, incidents can also be referred to Handsam Ltd, the Trust's appointed Data Protection Officer, for further guidance. Staff must not report directly to the Information Commissioner's Office (ICO). Instead, all breaches must first be logged via Handsam and reported to DSAMAT head office, who will assess the breach and determine whether it needs to be escalated to the ICO. This ensures consistent handling and expert input before any formal reporting is made.

21. Publication of information

- The Trust/school publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:
  - Policies and procedures
  - Minutes of meetings
  - Annual reports
  - Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The school / Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school / Trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. CCTV and photography

- DSAMAT and its Academies understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The school / Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
- Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All CCTV footage will be kept for 28 days for security purposes, unless required for evidential purposes, then this will be kept for 6 months. The headteacher is responsible (unless delegated to another member of staff) for keeping the records secure and allowing access.
- Viewing images for investigation is permitted only by the approval of a member of the Senior Leadership Team. Images will only be released to 3rd Parties if authorised by the Headteacher.
- All recordings of live lessons will be kept for six months for security purposes; the headteachers is responsible (unless delegated to another member of staff) for keeping the records secure and allowing access.
- The school / Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- If the school / Trust wishes to use images/video footage of pupils in a publication, such as the school / Trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.
- Precautions, as outlined in the DSAMAT e-safety policy, are taken when publishing photographs of pupils, in print, video or on the school website.
- Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.
- Parents and others attending school / Trust events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school / Trust.
- DSAMAT and its Academies asks that parents and others do not post any images or videos which include any children other than their own on any social media, or otherwise publish those images
- A log of access to CCTV footage must be maintained to ensure transparency and accountability. Any requests to view or access CCTV recordings must be formally logged using a CCTV Access Request Form (found at the end of this policy), which must be stored securely either in hard copy or in a digital format. This log should record the name of the requester, the reason for access, the date/time of access, and the

authorising staff member. This requirement should also be included on the list of compliance items to be monitored, as referenced on page 8 of this policy.

23. Cloud Computing

- For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.
- All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.
- If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.
- All files and personal data will be encrypted before they leave a school / Trust device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.
- As with files on school / Trust devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school / Trust should unauthorised access, deletion or modification occur and ensure ongoing compliance with the school's policies for the use of cloud computing.
- DSAMAT and its Academies usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the DSAMAT Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.

- Monitor the use of the school's / Trust's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher or line manager

24. Data retention

- The attached retention schedule (Pg 36) based on the IRMS toolkit for schools will be followed to ensure data us not kept for longer than is necessary
- Unrequired data will be deleted as soon as practicable.
- Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
- Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

25. DBS data

- All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- Data provided by the DBS will never be duplicated.
- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

26. Staff Training

All staff are required to complete the GDPR Data Protection course available on the Handsam portal to ensure a baseline understanding of their responsibilities under the UK GDPR and Data Protection Act.

In addition, managers and senior leaders may be required to undertake further data protection training, particularly where gaps in understanding are identified during internal reviews or visits. This will help ensure that those in leadership roles are confident in supporting data protection compliance across their schools.

Training needs will be kept under regular review to ensure ongoing awareness and compliance at all levels of the organisation.

27. Monitoring and Review

The Trust has delegated the responsibility for the implementation of this policy in discussion with the Data Protection Officer (DPO) to the Headteacher. The Trust will approve all major changes to this policy. The policy will be promoted and published throughout the Trust.

Appendix A: UK-GDPR To Do List

UK-GDPR TO DO LIST		
	TASK	**✓ / ✖**
1.	Review all data related policy and documentation.	
2.	Review data processing terms to ensure continued compliance.	
3.	Appoint a DPO where necessary. Or allocate new UK-GDPR responsibilities to a relevant individual with a clear allocation of responsibility.	
4.	Implement training and awareness raising programmes if required.	
5.	Review terms under which consent is gathered, ensuring compliance.	
6.	Ensure sufficient structures are in place to handle breaches, covering low and high risk, notification and response. Consult insurance cover on this point.	
7.	Review subject access requests procedures. Requests must be able to be responded to under the new rights, without charge and within the time limit.	
8.	Conduct a security audit, taking into account data protection by default and design for all forms of data storage and processing.	
9.	Is there a code of conduct or certification scheme active in the sector which can be consulted and adhered to?	
10	Review privacy/ fair processing notices ensuring the terms, format and content are a reflection of the UK-GDPR.	
11.	Formulate a Data Protection Impact Assessment and agree conditions under which it will be conducted within your organisation, assessing any applicable processes already underway and establishing a review structure.	
12.	Review marketing lists and processes to ensure they are capable of operating in compliance with the UK-GDPR right to object.	

Appendix B: Model Consent Request

Date:

Dear Sir or Madame,

(INSERT COMPANY/SCHOOL NAME) requires your freely given consent to proceed with the processing of your personal data. **(INSERT COMPANY/SCHOOL NAME)** will not proceed if you do not reply and will not take inaction as consent. **(INSERT COMPANY/SCHOOL NAME)** acknowledges that consent is not freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. The withdrawal of consent will generate no detriment to you as a subject. Consent will cover all processing activities carried out for the same purpose or purposes stipulated below. When the processing has multiple purposes, consent will be sought for them separately; group or omnibus consent is not valid.

*Please note: parental consent is required to process data of children under the age of 16 online. If you are completing this consent form for a child under 16, please tick the box below and your identity will then be verified.

The categories of personal data to which **(INSERT COMPANY/SCHOOL NAME)** will utilise are:

The above data will be processed for the following purposes:

Consent can be withdrawn quickly and easily in the following manner. **(PLEASE NOTE IF THE WITHDRAWAL OF CONSENT DOES NOT RENDER THE PROCESSING ILLEGAL)**:

If you have any questions you can contact our Data Protection Officer at **(OR INSERT ALTERNATIVE)**:

The Information Commissioner's Officer is our supervisory authority through which additional information can be sought, please also consult our online polices on data protection. Please retain for your records.

I consent to the stipulated use of the specified categories of personal data.

* I am completing this consent form on behalf of a data subject under the age of 16, and confirm I hold parental responsibility for said subject. (Please tick the box if relevant)			
Name:		**Signed:**	
Date:			

Appendix C: Privacy Notice Template

PRIVACY NOTICE		
Identity and contact details of controller:		
Contact details of Data Protection Officer (DPO):		
Statutory/contractual/condition of contract entry:		
Type of personal data concerned and origin of data: (If not secured directly from subject)		
Purpose of processing:		
Lawful basis for processing:		
Processing period/data retention:		
Rights under the UK-GDPR:	To be informed To object To restrict To erase	To rectify To portability To access
Recourse and complaints:		
Consequences of failure to provide and withdrawing consent:		
Recipient or categories of recipients of the personal data: (If any)		
Safeguards in place:		
Automated decision making framework and rationale: (If any)		

CCTV FOOTAGE REQUEST RECORD FORM
DA23

Appendix D: CCTV FOOTAGE REQUEST RECORD FORM

This checklist can be used to record any requests for CCTV footage, received by a school or college. A person should provide all the necessary information to assist the school in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school or college.

Any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. This must be requested in writing. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. If subject access request is received for surveillance footage or other information, unless an exemption applies, schools are required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data. This must be done by supplying them with a copy of the information in a permanent form. There are limited circumstances where this obligation does not apply. These include:

- Where the data subject agrees to receive their information in another way, such as by viewing the footage.
- Where the supply of a copy in a permanent form is not possible or would involve disproportionate effort.

The ICO's subject access code of practice makes clear this provision is only likely to be relevant in exceptional cases. If the data subject refuses an offer to view the footage or the data subject insists on a copy of the footage, then schools must consider ways in which we they can provide the data subject with this information.

More information on general personal data requests can be found on the ICO website: What is personal data?

Date/Time of Request	Person/s Requesting	Reason For Request & Footage Requested	Stored?	Agreed?	Date for Destruction	Released By	Camera/Location
			Y/N	Y/N			
			Y/N	Y/N			
			Y/N	Y/N			
			Y/N	Y/N			
			Y/N	Y/N			
			Y/N	Y/N			
			Y/N	Y/N			

Appendix E: Data Protection Impact Assessment Template

DATA PROTECTION IMPACT ASSESSMENT					
PROCESSING DETAILS					
SCALE, SCOPE AND CONTEXT	**PURPOSE AND PROCESSING OPERATION**	**NATURE OF PERSONAL DATA**	**PERIOD OF RETENTION**	**DATA ASSETS** e.g. networks or hardware	**COMPLIANCE WITH APPROVED CODES OF PRACTICE**

NECESSITY AND PROPORTIONALITY				
LAWFULNESS OF PROCESSING	**PRIOR CONSULTATION**	**DPO ADVICE**	**RISK TO RIGHTS AND FREEDOMS OF DATA SUBJECTS**	**LIKELIHOOD OF BREACH AND IMPACT (1-5)**

MANAGEMENT OF RISK			
MEASURES TAKEN TO REDUCE RISK	**COMPLIANCE DEMONSTRATION**	**DOCUMENTATION**	**MONITORING AND REVIEW**

Appendix F: Template Processing Log and Further Processing Rationale

PROCESSING LOG						
Name of controller/ processors	**Purpose of the processing**	**Categories of individuals and personal data**	**Retention schedules**	**Technical and organisational security measures**	**Categories of recipients of personal data**	**Consent**

FURTHER PROCESSING RATIONALE								
Original processing purpose and retention schedules	**New processing purpose**	**Links**	**Context in which data was collected**	**Categories of individuals and personal data**	**Consequence of further processing to subjects**	**Retention schedule amended**	**Technical and organisational security measures**	**Categories of recipients of personal data**

Appendix G: Legitimate Interest Assessment Template

LEGIMATE INTEREST ASSESSMENT				
Nature of processing	**Controller interests**	**Impact on the rights and freedoms of subjects**	**'Reasonably' expect data to be processed on this basis?**	**Implications for child data** (If applicable)

Appendix H: Internal Breach Register Template

INTERNAL BREACH REGISTER					
Date	**Details of breach**	**Consequences** (Subject and controller impact)	**Action taken**	**Timescale**	**Notification to authority and/or subject**

Appendix H: Data Protection and the Classroom: Managing the Human Factor

Over half of data breaches are as a result of human error. Handsam takes a look at a classroom corner to identify common data management errors and advise around preventing them.

Whiteboards provide a quick way to note down appointments; to jot down numbers and schedule out days but they are also highly visible to students, visitors and through windows and door glass. Think before you scribble down a piece of information on your whiteboard; is this personal or even sensitive personal data? Who will see it? Could it constitute a breach? The same best practice applies with interactive whiteboards. If the screen is up and active, freeze it and keep emails, file names and appointments from public view.

From having a password stronger than 1234 to not sharing your username, computer security is well known, but how well it is practised? Files should be stored securely, sensitive content encrypted, and password protected. User access should be limited to relevant data. Remember to lock computers when you leave the classroom and do not note down passwords on paper.

Files, memos and slips of paper left out on a desk are not secure and any personal data in this format is vulnerable to loss and breach. Keep memos generic; do not drop important forms or confidential documents on a colleague's desk in passing and have clear structures for how personal data moves around the school site.

Locked doors, secure windows, blinds and locks on draws seem like everyday features of modern classrooms and offices but you would be surprised how many function without these assets. A window which has been allowed to fall into disrepair or a door with a jammed lock is often overlooked. These features form key defences against data loss and bolster overall data security. It is easy to dash out without locking the door, but this could mean personal data is left exposed.

Appendix I: Breach Notification Supervisory Authority

BREACH NOTIFICATION SUPERVISORY AUTHORITY				
Controller name:				
DPO name and contact:				
Date and time of breach:				
Date and time of notification:				
Nature of breach:				
Categories of personal data affected:				
No. of subjects affected:				
No. of records affected:				
Subjects notified: (Communication affixed)	YES		NO	
	Reasons for non-notification:			
Potential and realised consequences:	(Cover subjects and controller)			
Security measures in place:				
Security measures to be implemented in response:				

Appendix J: Breach Notification Letter Template

Date:

Dear Sir or Madame,

(INSERT COMPANY/SCHOOL NAME) regret to inform you that despite the concerted efforts of our staff and the robust security measures in place, we have suffered a data protection breach involving elements of your personal data or that of a child dependent. The below notification informs you of the nature of the breach, the potential consequences and points of contact for any concerns you may have. We offer our sincerest apologies for this failure of data management and can assure you we are doing everything within our power to curb the negative effects. Please do not hesitate to approach us with concerns. The supervisory authority has been notified.

Yours sincerely,

Data controller **Data Protection Officer**

BREACH NOTIFICATION SUPERVISORY AUTHORITY	
Controller name:	
DPO name and contact:	
Date and time of breach:	
Date and time of notification to supervisory authority:	
Nature of breach:	
Categories of personal data affected:	
No. of subjects affected:	
No. of records affected:	
Potential and realised consequences:	(Cover subjects and controller)
Security measures in place:	
Security measures to be implemented in response:	

UK GDPR: retention and disposal of records (The Key, March 2025)

Statutory Retention Periods (based on the DfE Data Protection Guidance):

	Document Type	Retention Period	Action at the end of retention period	Guidance / Legislation
Child Protection Records	**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 (transferred separately from the main pupil file).	Store 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 and Working together to safeguard children.
Finance Records	**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	**Admissions**	6 years from the admission date.	Dispose of records securely.	Regulation 7 of the School Attendance (Pupil Registration) (England) Regulations 2024.
	Attendance registers	6 years from the date of entry.	Dispose of records securely.	Regulation 7 of the School Attendance (Pupil Registration) (England) Regulations 2024.
	Annual governors report	10 years.	Dispose of records securely.	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002. Retain as detailed in section 2 of the Limitation Act 1980.

	Document Type	Retention Period	Action at the end of retention period	Guidance / Legislation
Governance Records	**Curricular record**	At least 1 year.	Dispose of records securely.	The Education (School Records) Regulations 1989 and 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 – for the life of the academy plus 6 years • Annual reports – 10 years from the date of the report Board meeting records – 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 and the academy trust governance guide. Academy Trust Handbook

	Document Type	Retention Period	Action at the end of retention period	Guidance / Legislation
Health and Safety Records	**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 and 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 and Health surveillance – Record keeping.
	Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	The Regulatory Reform (Fire Safety) Order 2005. Retain as detailed in section 2 of the Limitation Act 1980.
Property Records	**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.

	Document Type	Retention Period	Action at the end of retention period	Guidance / Legislation
Pupil Records	**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 and 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.	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. See guidance on what to do if your school will close before the end of the retention period.
	Special educational needs and disabilities (SEND), including SEND statements and accessibility plans	6 years from the end of the EHC plan.	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.	See the SEND code of practice: 0 to 25 years. Retain as detailed in section 2 of the Limitation Act 1980. Transfer as detailed in Regulation 15 of The Special Educational Needs and Disability Regulations 2014.
Staff Records	**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.