THE DIOCESE OF GLOUCESTER ACADEMIES TRUST
unlocking potential

Data and Biometric Data Protection Policy

Our vision is to enable all to flourish.

Status and review cycle;	Statutory and annual
Responsible group:	The Trust Board
Implementation date:	May 2024
Reviewed date:	May 2026
Next review date:	May 2027

Contents

DBS data

Appendix 1 Data breach procedure

The Diocese of Gloucester Academies Trust employs SchoolPro TLC Ltd as its Data Protection Officer (DPO).

The DPO can be contacted on 01452 947633 or via email at dpo@schoolpro.uk

The Information Commissioner's Office can be contacted via the website: Information Commissioner's Office (ICO)

For general assistance, a suspected breach or a subject access request please contact the Trust in the first instance.

1.0 Statement of intent

1.1 The Diocese of Gloucester Academies Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under data protection legislation.

1.2 The Trust 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.

1.3 This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the UK GDPR.

2.0 Legal framework

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

- The General Data Protection Regulations (GDPR)
- The 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
- The School Standards and Framework Act 1998
- Protection of Freedoms Act 2012
- Electronic Commerce (EC Directive) Regulations 2022
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Keeping Children Safe in Education

2.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2024) 'Data Protection in Schools'
- DfE (2023) Generative artificial intelligence (AI) in education

2.3 Failure to comply with this policy may result in disciplinary action that may lead to dismissal and in addition the possibility of an individual being criminally prosecuted under the UK GDPR and the DPA and /or liable to pay compensation in any civil action.

3.0 Applicable data

3.1 For 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.

3.2 Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 2018. These specifically include the processing of:

- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Personal data which reveal:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade Union Membership

3.3 '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.

3.4 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.

3.5 In accordance with the requirements outlined in the UK GDPR, personal data will be managed adhering to the seven principles of the UK GDPR Regulation.

- Lawfulness, fairness and transparency

- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

3.6 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 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, whilst having regard to the purposes for which it is processed, to ensure that inaccurate data is 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 is 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 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.

3.7 The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4.0 Accountability

4.1 The Diocese of Gloucester Academies Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. and DPA, and will provide comprehensive, clear

and transparent privacy policies. The Trust will also provide evidence that it is complying with UK GDPR and DPA.

4.2 The Trust will be able to demonstrate how data is processed as a whole across the organisation, and will ensure each individual school within the Trust is adhering to the same procedure and that this is being implemented and enforced in line with the wider Trust policies.

4.3 Additional internal records of the Trust and school's processing activities will be maintained and kept up to date.

4.4 The Trust will provide comprehensive, clear and transparent privacy notices.

4.5 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories of data or information relating to criminal convictions and offences.

4.6 Internal records of processing activities (data flows) will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Details of consent
- 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 parties, including documentation of the transfer mechanism safeguards in place
- Data asset register
- Data Maps for processing activities
- Additional internal records of the school's processing activities will be maintained and kept up to date in Data flow

4.7 The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.

- Continuously creating and improving security features.

4.8 Data protection impact assessments will be used, where appropriate.

4.9 The DPO will conduct an annual audit of data processes.

5.0 Data protection officer (DPO)

5.1 A DPO will be appointed by the Trust to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Cooperate with the Information Commissioner's Office (ICO) and act as the first point of contact for the ICO and for individuals whose data is being processed.

5.2 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.3 The DPO will report to the highest level of management at the Trust, which is the Chief Executive Officer (CEO).

5.4 The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.5 Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

5.6 The DPO for the Trust is School Pro. TLC Ltd

6.0 Lawful processing

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

6.2 Under the GDPR Principles, Article 6, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for compliance with a legal obligation.
- 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 the performance of a contract with the data subject or to take steps to enter a contract for example recruitment or payroll.
- Processing is necessary for protecting the vital interests of a data subject or another person.
- 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 Trust in the performance of its tasks)
- 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)

6.3 Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject has been obtained
- 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:

  (a) Carrying out obligations under employment, social security or social protection law, or a collective agreement.

  (b) Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

  (c) The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

  (d) Reasons of substantial public interest based on Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.

  (e) 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.

  (f) Reasons of public interest in 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.

6.4 Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law.

6.5 When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data. The Trust will ensure that it and its schools have privacy notices established which clearly outline the reasons why it needs to collect personal data. The privacy notice will include the following explicit details:

- Why the school needs to collect personal data
- What the school plans to do with the personal data
- How long the school will keep the personal data
- Whether the school will share the personal data with any external organisations

6.6 The privacy notice will be clear and accessible to data subjects. The privacy notice will also be reviewed by the school's DPO at least annually and whenever significant changes are made to how the school processes the data that it collects.

6.7 The school will ensure that any parents, pupils and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which the school processes the data.

6.8 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.

7.0 Consent

7.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3 Where consent is given, a record will be kept documenting how and when consent was given. This will be kept in the school data asset register.

7.4 The Trust ensures that consent mechanisms meet the standards of 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.

7.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained. When pupils and staff join a school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

7.6 Consent can be withdrawn by the individual at any time.

7.7 The consent of parents will be sought prior to the processing of their data where appropriate

8.0 The right to be informed

8.1 The privacy notice supplied to individuals regarding the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.

8.2 If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3 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 (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal 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:

  (a) withdraw consent at any time.

  (b) 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.

8.4 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.

8.5 Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.6 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7 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 is disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

9.0 Subject Access Requests and Other Rights of Individuals

9.1 Individuals have the right to obtain confirmation that their data is being processed.

9.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data to verify the lawfulness of the processing.

9.3 The Trust will verify the identity of the person making the request before any information is supplied.

9.4 A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.7 All fees will be based on the administrative cost of providing the information.

9.8 All requests will be responded to without delay and at the latest, within one month of receipt.

9.9 In the event of numerous or complex requests, the period of compliance may be extended. 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.

9.10 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.11 Where a request is manifestly unfounded or excessive, the 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.

9.12 The Trust 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 Trust will:

9.13 Omit certain elements from the response if another individual's personal data would be disclosed otherwise.

9.14 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.

9.15 Explain to the individual who made the SAR why their request could not be responded to in full.

9.16 If a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

9.17 To request access to data, subjects should contact the headteacher of the relevant school or if the data is held centrally by the Trust, the CEO.

9.18 On receiving a Subject Access Request, the request must be forwarded it to the Trust's DPO for validation and support. The Estates and Compliance Manager must be informed, and the request must be recorded and uploaded via the SchoolPro reporting portal or using GDPR@SchoolPro.uk

10.0 Responding to Subject Access Requests

10.1 When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

10.2 We will not disclose information if it:

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

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

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

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

10.6 The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- It is the third party's responsibility to provide evidence of this entitlement.
- This might be a written authority to make the request, or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if we can contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

11.0 The right to rectification

11.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2 Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

11.3 Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the 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. The Trust reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

11.4 The Trust will take reasonable steps to ensure that data is accurate or is 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. The Trust will restrict processing of the data in question whilst its accuracy is being verified, where possible.

11.5 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

11.6 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

11.7 Where no action is being taken in response to a request for rectification, the 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.

12.0 The right to erasure

12.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling or legal reason for its continued processing.

12.2 Individuals 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
- 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 to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

12.3 The Trust will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

12.4 The 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

12.5 The establishment, exercise or defence of legal claims

12.6 The 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.

12.7 Requests for erasure will be handled free of charge; however, the 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.

12.8 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.

12.9 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.

12.10 Where personal data has been made public within an online environment, the Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13.0 The right to restrict processing

13.1 Individuals have the right to block or suppress the Trust's processing of personal data.

13.2 If processing is restricted, the 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.

13.3 The Trust 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 Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the 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 Trust no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

13.4 If the personal data in question has been disclosed to third parties, the 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.

13.5 The school 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.

13.6 The Trust will inform individuals when a restriction on processing has been lifted.

14.0 The right to data portability

14.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

14.2 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.

14.3 The right to data portability only applies in the following cases:

- To personal data that an individual has provided 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

14.4 Personal data will be provided in a structured, commonly used and machine-readable form.

14.5 The Trust will provide the information free of charge.

14.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7 The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8 If the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

14.9 The Trust will respond to any requests for portability within one month.

14.10 Where the request is complex, or several 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.

14.11 Where no action is being taken in response to a request, the 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.

15.0 The right to object

15.1 The Trust will inform individuals 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.

15.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

15.3 Where personal data is processed for the performance of a legal task or legitimate interests:

15.4 An individual's grounds for objecting must relate to their situation.

- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.5 Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The 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.

15.6 Where personal data is processed for research purposes:

- The individual must have grounds relating to their situation to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

15.7 Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online. 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. The Trust 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.

15.8 Where no action is being taken in response to an objection, the 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.

16.0 Automated decision-making and profiling

16.1 Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2 The Trust 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.

16.3 When automatically processing personal data for profiling purposes, the 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.

16.4 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest based on Union/Member State law.

17.0 Data protection by design and default

17.1 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 (DPIAs) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process – see section 14.1)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

17.2 A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project. We will undertake a DPIA for processing that is likely to result in a high risk to individuals as well as any other major project which requires the processing of personal data.

17.3 It is vital that the DPIA is completed before processing is commenced to ensure that all risks are identified and mitigated as much as possible.

17.4 Our DPIA will:

- describe the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

17.5 To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. We will consult our data protection officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors. If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing. We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

18.0 Data breaches

18.1 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.

18.2 For the central team, the COO and DPO will ensure that all central staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training, this may include induction.

18.3 For school staff, the headteacher and DPO will ensure that staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training, this may include induction.

18.4 All data breaches must be treated as per the guidance in this document. (Refer to Appendix 1 data breach procedure.)

18.5 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.6 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Trust becoming aware of it.

18.7 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.

18.8 If a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust will notify those concerned directly.

18.9 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.10 If a breach is sufficiently serious, the public will be notified without undue delay.

18.11 Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.12 Within a breach notification, 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

18.13 Where notifying an individual about a breach to their personal data, the school 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. The

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.

19.0 Data security

19.1 The security of personal data is of utmost importance and as outlined in Article 5 (1) (f) of the UK GDPR the Trust ensures the appropriate security of personal data including to avoid the accidental loss, damage or destruction of data.

19.2 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access and will not be left unattended or in clear view anywhere with general access.

19.3 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.

19.4 All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.5 Unless safeguards are in place and approved by the school, staff will not use their personal laptops or computers for Trust purposes Trustees and local governors will not use their personal laptops or computers for Trust purposes unless they are password-protected. All Trustees and local governors will be provided with a secure trust e-mail account which should be used for all trust communications.

19.6 All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.7 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.

19.8 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, extra care will be taken to follow the same procedures for security, e.g. keeping devices under lock and key. Taking such information off the premises should be kept to an absolute minimum, however personnel files and children's safeguarding records must not be removed from the premises unless it is being transported to a new setting. The person taking the information from the Trust premises accepts full responsibility for the security of the data.

19.9 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.

19.10 Under no circumstances are visitors allowed access to confidential or personal information unless legally obliged, suitable due diligence has been carried out or a data sharing exercise is in place. Visitors to areas of the Trust containing sensitive information must be always supervised.

19.11 The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

19.12 The Trust takes its duties under the GDPR seriously and any unauthorised disclosure or a loss of data may result in disciplinary action.

19.13 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. 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.

19.14 The Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we may seek consent, if necessary, before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT and communication companies, education support companies, and those that provide tools for learning.

19.15 When doing this, we will:

19.16 Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

19.17 Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

19.18 Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

19.19 Share personal data with law enforcement and government bodies where we are legally required to do so, including for:

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

19.20 We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff. We may share data in appropriate legal circumstances to the data subjects nominated power of attorney.

19.21 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

19.22 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. This is except for data that is retained in the school archive as described in section 15. 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's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19.23 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is secured securely and adequately protected.

20.0 Password procedures

20.1 Password length and creation

Passwords used to access school computers, laptops and other electronic devices should follow the NCSC "three random words" approach. This means creating a password from three unrelated words, resulting in a long, strong and memorable passphrase (typically).

- No mandatory regular password changes
- Staff and pupils should not be required to change passwords at regular intervals unless there is evidence or suspicion of a security breach. The focus should be on creating a strong, unique password rather than frequent changes.

20.2 Safe password practices

- Passwords must not be shared with anyone.
- Avoid using personal information (such as names, dates of birth, or common words).
- Using a passphrase based on three random words makes passwords easier to remember and harder for attackers to guess.

20.3 Use of password managers

- Staff are encouraged to use the Microsoft office password manager to securely store and manage passwords, allowing unique and strong passwords to be used for each system without the need to memorise them all.

20.4 Additional recommendations

20.4.1 Where available, multi-factor authentication (MFA**)** should be enabled to give additional protection against unauthorised access.

21.0 Safeguarding

21.1 The Trust understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe. The school 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.

21.2 The 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

21.3 The school 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.

The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

22.0 Publication of information

22.1 The Trust publishes a Freedom of Information Publication Scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

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

22.3 The Trust and its individual schools will not publish any personal information, including photos, on its website without the permission of the affected individual or if it is a child their parents.

22.4 When uploading information to the Trust or school websites, staff will be considerate of any administrative metadata or deletions which could be accessed in documents and images on the site. Metadata is data about data and in the context of this policy, metadata refers to any digital records that are primarily for administrative purposes but include personal data. E.g. the titling of photographs, indexing of electronic articles or web pages.

23.0 CCTV and Photography

23.1 The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

23.2 Individual schools will notify pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

23.3 Cameras will only be placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

23.4 CCTV footage will be kept for six months for security purposes.

23.5 As part of our school activities, we may take photographs and record images of individuals within our schools. We will not seek consent from parents/carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and school displays. We will process these images under the legal basis of Public Task. We will obtain written consent from parents/carers for

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

23.6 Uses may include:

- Within school on public area 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

23.7 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.

23.8 When using photographs and videos in this way we will not usually accompany them with any other personal information about the child, to ensure they cannot be identified.

24.0 Biometric recognition systems

St John's C of E Academy does not collect or otherwise process biometric data.

25.0 Cloud computing

25.1 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.

25.2 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.

25.3 If the cloud service offers an authentication process, each user will have their own account. The Trust will implement a system 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.

25.4 All files and personal data will be encrypted before they leave a school 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.

25.5 Only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur and ensure ongoing compliance with the school's policies for the use of cloud computing.

26.0 Data retention

26.1 Data will not be kept for longer than is necessary and unrequired data will be deleted as soon as practicable.

26.2 Some educational records relating to former pupils or employees of the Trust 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.

27.0 DBS data

27.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

27.2 Schools do not have to keep copies of DBS certificates to fulfil the duty of the requirements of the Data Protection Act. A copy of the other documents used to verify the successful candidate's identity, right to work and required qualifications should be kept for the personnel file. 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.

Appendix 1

Personal Data Breach Procedure

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

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the headteacher, or in the case of the central team, their line manager.

The headteacher or line manager will investigate the report and determine whether a breach has occurred. To decide, the headteacher or line manager will liaise with the DPO to consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The headteacher or line manager will seek advice from the DPO.

The headteacher or line manager will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the DPO and relevant staff members or data processors where necessary. (actions relevant to specific data types are set out at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen based on the headteacher or line manager's initial investigation and will advise the headteacher further.

The DPO in conjunction with the headteacher or line manager, will determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identity theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO

will notify the ICO.

The headteacher or line manager will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Breach-Log document in electronic format. · Where the ICO must be notified, the DPO or Headteacher/line manager will do this via the 'report a breach' page of the ICO website. As required, the report 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 all the above details are not yet known, the Trust will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information. The Headteacher, line manager or DPO will submit the remaining information as soon as possible.

The school will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the school or Trust will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The school or Trust will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The Trust 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 are in the Breach-Log document in electronic format.

The DPO and headteacher or line manager will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

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

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

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

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach might include:

- Details of pupil premium children being published on the school website
- Non-anonymised pupil data or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.