



# Data Protection Policy

(GDPR Compliant)

Incorporating Biometric Data Policy

Our vision is to enable all to flourish.

Status and review cycle;	Statutory and annual
Responsible group:	The Trust
Next Review Date:	August 2024

## Contents

### **Statement of intent**

1. **Legal framework**
2. **Applicable data**
3. **Principles**
4. **Accountability**
5. **Data protection officer (DPO)**
6. **Lawful processing**
7. **Consent**
8. **The right to be informed**
9. **The right of access**
10. **The right to rectification**
11. **The right to erasure**
12. **The right to restrict processing**
13. **The right to data portability**
14. **The right to object**
15. **Automated decision making and profiling**
16. **Privacy by design and privacy impact assessments**
17. **Data breaches**
18. **Data security**
19. **Publication of information**
20. **Photography and CCTV**
21. **Cloud computing**
22. **Data retention**
23. **DBS data**
24. **Glossary**

**Appendix 1 Data breach procedure**

**Appendix 2 Impact assessment template**

**Biometric Data Policy**

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

The Trust's named Data Protection Officer is Richard Morley who can be contacted on [rmorley@schoolpro.uk](mailto:rmorley@schoolpro.uk) or via telephone number **0203 2909093**

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

## **Statement of intent**

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 the General Data Protection Regulation (GDPR). The General Data Protection Regulation 2018 (GDPR) is a set of rules designed to make sure that people's personal data is kept safe and is not used inappropriately.

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.

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 GDPR.

## **1.0 Legal framework**

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

- The General Data Protection Regulation (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 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

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

- Information Commissioner's Office (2021) 'Guide to the UK General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'

1.3 This policy will be implemented in conjunction with the following other Trust policies:

- Recruitment and selection
- Reference Policy
- Equal Opportunities
- Disciplinary Policy
- Freedom of Information
- Health and Safety
- Social Media Policy

## **2.0 Applicable data**

2.1 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 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.

2.2 Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. 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 reveals
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Principles

### **3.0 Principles**

3.1 In accordance with the requirements outlined in the 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, 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.

3.2 The 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 GDPR.

4.2 The Trust will provide comprehensive, clear and transparent privacy policies.

4.3 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.

4.4 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
- Additional internal records of the school's processing activities will be maintained and kept up to date.

4.5 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.

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

4.7 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 in order 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, data will be lawfully processed under the following conditions:
  - (a) The consent of the data subject has been obtained.
  - (b) Processing is necessary for compliance with a legal obligation.
  - (c) 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.
  - (d) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract for example recruitment or payroll.
  - (e) Processing is necessary for protecting the vital interests of a data subject or another person.
  - (f) 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)
- 6.3 Sensitive data will only be processed under the following conditions:
  - Explicit consent of the data subject has been obtained, unless reliance on consent is prohibited by EU or Member State law.
  - 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 on the basis of 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 on the basis of Union or Member State law or a contract with a health professional.
- (f) 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.
- (g) Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

## **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 the 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.
- 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 in regards to 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 The right of access**

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 in order 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 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.

9.10 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.

- 9.11 In the event that 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.
- 9.12 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.
- 9.13 On receiving a Subject Access Request, headteachers must forward to the Trusts DPO for validation and support. The CEO must be informed and also the request must be recorded and uploaded via the SchoolPro reporting portal or using [GDPR@SchoolPro.uk](mailto:GDPR@SchoolPro.uk)

## **10.0 The right to rectification**

- 10.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- 10.2 Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.
- 10.3 Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.
- 10.4 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 10.5 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.

## **11.0 The right to erasure**

- 11.1 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.
- 11.2 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 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
- 11.3 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
- The exercise or defence of legal claims

11.4 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.

11.5 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.

11.6 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.

## **12.0 The right to restrict processing**

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

12.2 In the event that 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.

12.3 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

12.4 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.

12.5 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.

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

## **13.0 The right to data portability**

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

13.2 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.

13.3 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
- 13.4 Personal data will be provided in a structured, commonly used and machine- readable form.
- 13.5 The Trust will provide the information free of charge.
- 13.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- 13.7 The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 13.8 In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.
- 13.9 The Trust will respond to any requests for portability within one month.
- 13.10 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.
- 13.11 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.

#### **14.0 The right to object**

- 14.1 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.
- 14.2 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.
- 14.3 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 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.
- 14.4 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.

- 14.5 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 Trust is not required to comply with an objection to the processing of the data.
- 14.6 Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

## **15.0 Automated decision making and profiling**

- 15.1 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.
- 15.2 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.
- 15.3 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.
- 15.4 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 on the basis of Union/Member State law.

## **16.0 Privacy by design and privacy impact assessments**

- 16.1 The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.
- 16.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.
- 16.3 DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur.
- 16.4 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.

16.5 A DPIA could be used for more than one project, where applicable.

16.6 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.

16.7 The Trust 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

16.8 Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

16.9 A Trust impact assessment template is provided at Appendix 2 of this document.

16.10 Trust central staff are available to support with the completion of a DPIA.

## **17.0 Data breaches**

17.1 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.

17.2 For the central team, the CEO 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.

17.3 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.

17.4 All Data Breaches must be treated as per the guidance in this document. (Refer to Appendix I data breach procedure.)

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

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

17.7 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.

17.8 In the event that 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.

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

17.10 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

- 17.11 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.
- 17.12 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
- 17.13 The Trust's data breach procedure is Appendix I of this document.

## **18.0 Data security**

- 18.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- 18.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.
- 18.3 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.
- 18.4 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.
- 18.5 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- 18.6 All electronic devices are password-protected to protect the information on the device in case of theft.
- 18.7 Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 18.8 Unless safeguards are in place and approved by the school, staff will not use their personal laptops or computers for Trust purposes.
- 18.9 Trustees and Governors will not use their personal laptops or computers for Trust purposes unless they are password-protected. All Trustees and Governors will be provided with a secure trust e-mail account which should be used for all trust communications.
- 18.10 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- 18.11 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- 18.12 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 18.13 When sending confidential information by fax, staff will always check that the recipient is correct before sending.

- 18.14 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. Taking such information off the premises should be kept to an absolute minimum, however personnel files and children's safeguarding records should 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.
- 18.15 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.
- 18.16 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 supervised at all times.
- 18.17 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.
- 18.18 The Diocese of Gloucester Academies Trust takes its duties under the GDPR seriously and any unauthorised disclosure or a loss of data may result in disciplinary action.

## **19.0 Safeguarding**

- 19.1 The Trust understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.
- 19.2 The school 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
- 19.3 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.

## **20.0 Publication of information**

- 20.1 The Diocese of Gloucester Academies Trust 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

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

20.3 The Diocese of Gloucester Academies 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.

20.4 When uploading information to the Trust or school websites, staff are 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.

## **21.0 CCTV and Photography**

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

21.2 The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

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

21.4 The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

21.5 If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust/school websites, prospectus, or recordings of plays, written permission will be sought for the particular usage from the parent of the pupil.

21.6 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

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

## **22.0 Cloud computing**

22.1 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.

22.2 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.

- 22.3 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.
- 22.4 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.
- 22.5 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.
- 22.6 The Trust's / school's 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.
- 22.7 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 school's 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 cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher.

## **23.0 Data retention**

- 23.1 Data will not be kept for longer than is necessary.
- 23.2 Unrequired data will be deleted as soon as practicable.
- 23.3 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.
- 23.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.
- 23.5 For further guidance please refer to the Trust's Data Retention Policy.

## **24.0 DBS data**

- 24.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- 24.2 Schools do not have to keep copies of DBS certificates in order to fulfil the duty of the requirements of the Data Protection Act, when a school or college chooses to retain a copy, it should not be retained for longer than six months. 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
- 24.3 Data provided by the DBS will never be duplicated.
- 24.4 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.

## **25.0 Training and Development**

- 25.1 The Trust is committed to ensuring the staff adopt the highest standards in relation to the processing and handling of personal data.
- 25.2 All existing staff will be trained within 6 months of the dissemination of this Policy.
- 25.3 New staff will be trained within 3 months of their joining the Trust and being able to access Personal Data. This policy will form part of their induction pack.
- 25.4 Staff will be re-trained according to their needs against the tide of new guidance and legislation. It is anticipated that this will usually be annually.
- 25.5 No member of staff will have access to any personal data unless they have read this Policy first.

## **26.0 Glossary**

Data Protection Act 1998 ("DPA")	The law on data protection in the UK
General Data Protection Regulation ("GDPR")	A new law on data protection that comes into force on 25 May 2018 throughout Europe
Data Controller	A person or organisation that handles and processes personal data and determines the way such data should be processed
Department for Education ("DfE")	The government department with regulatory powers
Metadata	Data that is about data. As an example, cataloguing of records or indexing of files. It can be both electronic or paper based.
Personal Data	Any information from which a living individual can be identified
Sensitive Personal Data	Any Personal Data which includes further information as defined in the DPA. Further

information includes (i) racial or ethnic origin; (ii) political opinions; (iii) religious beliefs; (iv) membership of a trade union; (v) physical or mental health or condition; (vi) sexual life or preferences; (vii) information about any criminal offence or court proceedings related to a criminal offence

Information  
Commissioner's Office  
("ICO")

The statutory regulator of the DPA and the  
GDPR

Privacy Notice

A description of Personal Data held by the  
Trust, along with details of purpose, retention  
and other information about how the Trust  
will handle the Personal Data

Data Subject

As defined in the DPA and the GDPR. The  
Data Subject is the person who the Personal  
Data is about, or who is identified by the  
Personal Data

Data Privacy Impact  
Assessments ("DPIAs")

The new requirement under the GDPR to  
impact assess all Personal Data that is held and  
record all processing activities

# Appendix I

## Data Breach Procedure

***For the purposes of this procedure “Trust” refers to the Diocese of Gloucester Academies Trust and all of its member schools.***

The Diocese of Gloucester Academies Trust holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost, stolen or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by the Trust and all of its staff, trustees, governors, volunteers and contractors, referred to herein after as 'staff'.

### **Purpose**

This breach procedure sets out the course of action to be followed by all staff within the Trust if a data protection breach takes place.

### **Types of Breach**

Data protection breaches could be caused by a number of factors. A number of examples are shown below.

- Loss or theft of pupil, staff or governing body data and / or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Poor data destruction procedures;
- Human error;
- Cyber-attack;
- Hacking.

### **Managing a Data Breach**

In the event that the Trust identifies or is notified of a personal data breach, the following steps must be followed:

- In a DGAT school, the person who discovers/receives a report of a breach must inform the headteacher or, in their absence the deputy headteacher. In the case of central staff identifying a data breach, this must be reported to the CEO in line with this policy. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. On receipt of the notification the headteacher will inform the Trusts' Head of Business and Operations and in their absence the CEO. The Trust will inform the Data Protection Officer (DPO). For data breaches related to the central team, the CEO will inform the DPO and Head of Business and Operations.
- The school must register the breach via the SchoolPro reporting portal or using [GDPR@SchoolPro.uk](mailto:GDPR@SchoolPro.uk)
- The headteacher, or in the case of the central team, the CEO, with the assistance of the DPO should ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT support provider.
- The DPO will support the school or Trust and will advise on whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

- The DPO will advise and assist the headteacher or CEO to take appropriate steps to recover any losses and limit the damage. Steps might include:
  1. Attempting to recover lost equipment.
  2. Contacting any relevant 3<sup>rd</sup> party organisations, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff.

The use of back-ups should be implemented to restore lost/damaged/stolen data.

If bank details have been lost or stolen, consider contacting banks directly for advice on preventing fraudulent use.

If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

## **Investigation**

In most cases, the next stage would be for the headteacher or CEO to fully investigate the breach with the support of the DPO. The headteacher, or CEO in the case of data breaches related to the central team, with the assistance of and cooperation of the DPO, Trust and the school will ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record will be made of the nature of the breach and the actions taken to mitigate it. The investigation will be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

## **Notification**

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO will, after seeking expert or legal advice, advise the Trust whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis. Where notification is required to be given, the DPO and Trust central team will support the school to complete this requirement.

Should the breach lead to a complaint this will be fully investigated with the support of the DPO and any findings or actions communicated to the complainant in line with the complaints policy. If the complainant is unhappy with the outcome of the investigation they should be advised that there recourse to advice or further complaint is via the Information Commissioner's Office.

## **Review and Evaluation**

Once the above steps have been completed and the breach is over, the DPO will support the headteacher or CEO in a full review of both the causes of the breach and the effectiveness of the response to it. The report will be made available to the headteacher and also the CEO of the Trust and is required to be reported to the Trust Board.

If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Trust for advice and guidance.

This breach procedure will be reviewed after a breach occurs or after legislative changes, new case law or new guidance.

## **Implementation**

The headteacher, or for central staff members, the CEO, should ensure that all staff are aware of the Trust's Data Protection Policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Trust's Data Protection Policy and associated procedures, they should discuss this with their line manager, DPO or the headteacher.

## Appendix 2

### Data protection impact assessment (DPIA)

As part of Trust's responsibility under the GDPR, schools should conduct a DPIA in the following circumstances:

- When using new technologies.
- If the data processing is likely to result in a high risk to the rights and freedoms of individuals

DPIAs allow schools to identify privacy risks posed to individuals in certain situations, and establish effective control measures, ensuring they comply with the principles of the GDPR and meet individuals' expectations of privacy. Conducting a DPIA at an early stage ensures that measures are in place – minimizing the data protection risks of processing activities.

Submitting Controller Details			
Name of controller			
Reason for DPIA			
Name of DPO	SchoolPro TLC Limited		
Step 1: Project Description			
Explain broadly what project aims to achieve and what type of processing it involves.			
Step 2: Processing			
About the handling of the data – How will you collect, use, share, store and delete data?			
About the data – quantity of data, timeframe, and type. reference special category data.			
About the data subjects – Expectations and control? Reference vulnerable groups and existing concerns over current processing.			
Identify benefits of the processing.			
Step 3: Consultation			
How will you consult with relevant stakeholders, or why not appropriate?			
Step 4: Compliance Consideration			
Describe compliance and proportionality measures.			
Step 5: Identify and Assess Risks			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm L/M/H	Severity of harm L/M/H	Overall risk L/M/H



<b>Step 6: Identify Measures to Reduce Risk</b>				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5.				
Risk	Options to reduce or eliminate risk	Risk Eliminated, Reduced, Accepted.	Residual risk L/M/H	Measure approved Yes / No
<b>Step 7: Sign Off and Record Outcomes</b>				
Item	Name/position/date	Notes		
Measures approved by:		Note actions and responsibilities for compliance with DPIA		
Residual risks approved by:		Consult with ICO before going ahead if High risk remains		
DPO advice provided:				
DPO advice:				
DPO advice accepted or overruled:		If overruled, give reasons		
Comments:				
Consultation responses reviewed by:		If decision making is not in line with consultation, give reasons		
Comments:				
This DPIA will kept under review by:				
Additional Notes:				

# Biometric Data Policy

## 1.0 What is Biometric Data?

- 1.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.
- 1.2 Schools that use pupils' biometric data must treat the data collected with appropriate care and must comply with the data protection principles as set out in the General Data Protection Regulation 2018.
- 1.3 The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulation 2018; this means that it must be obtained, used and stored in accordance with the Regulation.
- 1.4 Personal data used as part of an automated biometric recognition system must also comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.
- 1.5 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools, academies and colleges when used as part of an automated biometric recognition system.
- 1.6 Schools must ensure that the parent/carer of each pupil is informed of the intention to use the pupil's biometric data as part of an automated biometric recognition system. Parents/carers must be advised that alternative methods to biometric scanning are available for processing identity if required.
- 1.7 The written consent of the parent/carer or the pupil, where the pupil is deemed to have the capacity to consent, must be obtained before the data is taken from the pupil and processed within the biometric recognition system. In no circumstances can a pupil's biometric data be processed without written consent.
- 1.8 Schools must not process the biometric data of a pupil where:
  - a) the pupil (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
  - b) a parent or pupil has not consented in writing to the processing; or
  - c) a parent or pupil has objected in writing to such processing, even if another parent has given written consent.
- 1.9 Schools must provide reasonable alternative means of accessing the services to those pupils who will not be using an automated biometric recognition system.

## 2.0 Biometric Data and Processing

### 2.1 What Is an Automated Biometric Recognition System?

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed above.

## 2.2 What Does Processing Data Mean?

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it.

An automated biometric recognition system processes data when:

- a) recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- b) storing pupils' biometric information on a database system; or
- c) using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

## 2.3 Who Is Able to Give Consent?

The Data Protection Act gives pupils rights over their own data when they are considered to have adequate capacity to understand. Most pupils will reach this level of understanding at around age 13.

For this reason, for most pupils in a secondary school, it will normally be up to the individual pupil to decide whether or not to provide biometric data. Where the school considers that the pupil does not have the capacity, or they are under the age of 13, parents/carers will be asked to provide written consent.

## 2.4 Alternative to Biometric

The school or school will provide an alternative to biometric scanning for any parent/pupil objecting to the processing of biometric data.

## 2.5 Length of Consent

The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/carer or the pupil themselves objects to the processing (subject to the parent's/carer's objection being in writing).

When the student leaves the school or school, their biometric data will be securely removed from the school's biometric recognition system.