Bradford Diocesan Academies Trust

GENERAL DATA PROTECTION REGULATION (G.D.P.R.) POLICY

Issued: April 2018
Next Review Due: July 2019

Bradford Diocesan Academies Trust

Summary of differences.

1. This policy refers to the GDPR over the Data Protection Act 1998
2. Definitions of Personal and Sensitive Personal Data have been included to help staff identify what counts.
3. The requirements of the trust to document and audit our processing activities has been included.
4. The specific legal bases upon which we must rely to process personal data has been included, again to make it easier for staff to understand when they can do so.
5. Consent and the specific restrictions around it has been included.
6. The rights of a data subject to object, to data portability and to restrict processing have been added.
7. Much greater detail has been included in the data security section.
8. The principles of Data Protection by Design and Impact Assessments have been included.
9. An outline of the Trusts procedure on dealing with breaches of personal data has been included.

1. Introduction

1.1 This policy sets out how the Bradford Diocesan Academies Trust (the "Trust") handles the personal data of its students, students' parents, employees, workers, contractors, suppliers and other third parties.

2. Legal framework

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

- The General Data Protection Regulation (GDPR) 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Trust Standards and Framework Act 1998
- The Data Protection Bill 2018 in its current form.

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

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR).
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3. Applicable data

3.1 For the purpose of this policy, **personal data** refers to any 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.

3.2 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 personal data revealing sexual orientation or activities, racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data and data concerning health matters.

4. Principles

4.1 In accordance with the requirements outlined in the GDPR, personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the 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.

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

5. Accountability

5.1 The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in compliance with the principles set out in the GDPR.

5.2 The Trust will provide comprehensive, clear and transparent privacy policies for both our workforce and student population.

5.3 Additional internal records of the Trust's processing activities will be maintained and kept up-to-date in the Trust's Information Asset Register.

5.4 Internal records of processing activities will include the following:

- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Third party recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- Legal basis for the processing

5.5 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.

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

6. Data protection officer (DPO)

6.1 A DPO has been appointed 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.

6.2 The Director of Operations has been appointed to the role of DPO on the grounds that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

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

6.4 The DPO will report to the highest level of management at the Trust, which is the Board of Trustees and the Chief Executive Officer.

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

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

6.7 Each BDAT academy is to appoint a Data Protection Coordinator (DPC) who will be the central point of contact with the academy for data protection issues. Staff will be made aware of who the person is.

7. Lawful processing

7.1 The legal basis for processing data must be identified and documented in the Trust's and Academy's Information Asset Register prior to data being processed.

7.2 Under the GDPR, data can only 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.
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - For the performance of a contract with the data subject or to take steps to enter into a contract.
    - Protecting the vital interests of a data subject or another person.

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

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.

- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

8. Consent

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

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

8.3 Where consent is given, a record will be kept documenting how and when consent was given.

8.4 The Trust will ensure that consent mechanisms meet the standards of the GDPR. Where these standards cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

8.5 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.

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

8.7 Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed

9.1 Privacy notices will be supplied to members of the workforce and students (and their Parents/Guardians where appropriate) at the time they join the Trust, and be available online at the Trust's website. (link to be inserted)

9.2 Privacy notices will be written in clear, plain language which is concise, transparent, easily accessible and will be supplied free of charge.

9.3 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.

9.4 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:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.

9.5 Where appropriate, the existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences. 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.

9.6 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.

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

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

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

10. The right of access

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

10.2 Individuals have the right to submit a subject access request (SAR) to gain access to their Personal data.

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

10.4 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.

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

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

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

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

10.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

10.10 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.

11. 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 Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

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

11.5 Where the Trust decides not to action for rectification, the Trust will explain the reason for this to the individual, and will inform them of their right to complain to the ICO and to a judicial remedy.

12. The right to erasure

12.1 Individuals have the right to request the deletion or removal of personal data 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, and that consent was the only legal basic for the continued processing of that data.
- 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

12.2 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 archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

12.3 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.

12.4 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.

12.5 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 The right to restrict processing

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

13.2 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.

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

14 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 in the following circumstances:

- In relation 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

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

14.3 Personal data will only be provided after appropriate verification of the identity of the requester has been carried out.

14.4 The Trust will provide the information free of charge.

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

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

14.7 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.

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

14.9 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.

14.10 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 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:

- 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.

15.4 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.

15.5 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.

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

16 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

16.5 Automated decision making must not 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.

17 Privacy by design and privacy impact assessments

17.1 The Trust will adopt a privacy by design approach and implement technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

17.2 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.

17.3 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.

17.4 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.

17.5 A DPIA will be used for more than one project, where necessary.

17.6 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.

17.7 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 assessment of the risks to individuals
- The measures implemented in order to address risk.

17.8 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.

18 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 The Data Protection Officer will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Trust will report the breach to the Information Commissioner's Office (ICO).

18.4 All notifiable breaches will be reported to the ICO within 72 hours of the Trust becoming aware of it.

18.5 The need to notify the ICO, will be assessed on a case-by-case basis.

18.6 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.

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

18.8 The Trust will implement effective and robust breach detection, investigation and internal reporting procedures, which facilitate decision-making in relation to whether the ICO or the public need to be notified.

18.9 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

19 Data security

19.1 Confidential paper records must be stored in a locked filing cabinet, drawer or safe, with restricted access. Confidential paper records must not be left unattended or in clear view anywhere with general access.

19.2 Digital data stored on-site is regularly backed up off-site.

19.3 Removable media such as USB drives and portable hard drives will not be used to hold personal information unless they are password-protected and fully encrypted.

19.4 All computing equipment must be password-protected to protect the information on the device from unauthorised access. All portable computing equipment, for example laptops, must be encrypted.

19.5 Where possible, the Trust will remotely block or delete personal data (for which the Trust is the data controller) stored on an electronic device in case of theft or if the device is the personal equipment of an employee who is leaving the Trust's employment. To facilitate this, Staff and governors wishing to access their Trust email account via a mobile device must only do so using either a web browser or via the Microsoft Outlook Application.

19.6 Staff and governors must not store (I.E. download or save on to) personal data for which the Trust is the data controller on their personal laptops or computers (including mobile phones).

19.7 Staff and governors must not use **personal** cloud storage systems (e.g. Dropbox, Box, Google Drive) to store or transfer data. The use of a Trust or school implemented system is permitted.

19.8 Emails containing sensitive or confidential information must be protected. Trustees and Governors will only be communicated with via Trust or school email addresses; the Trust will not send emails to personal email addresses.

19.9 The Trust will ensure circular emails to parents are sent blind carbon copy (bcc), so that personal email addresses are not disclosed to other recipients.

19.10 When sending confidential information by fax or email, staff will always check that the recipient is correct before sending.

19.11 Where personal data is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data. No electronic data should be taken off premises unless the device it is stored upon is encrypted.

19.12 Before sharing data with third parties, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The recipient of the data has been outlined in a privacy notice.

19.13 Under no circumstances are visitors allowed access to personal data. Visitors to areas of the Trust containing personal data will be supervised at all times.

19.14 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.

20 Publication of information

20.1 The Trust will publish 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 Trust will not publish any personal information, including photos, on its website without the consent of the individual concerned.
20.4 When uploading information to the Trust website, staff are considerate of any deletions which could be accessed in documents and images on the site.

21 CCTV and photography

21.1 Recording images of identifiable individuals constitutes processing personal data, so such processing will be carried out in line with data protection principles.
21.2 The Trust will notify all students, staff and visitors of the purpose for collecting CCTV images via privacy notices.
21.3 Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
21.4 All CCTV footage will be kept in accordance with the retention schedule. The Business Manager is responsible for keeping the records secure and allowing access.
21.5 The Trust will always indicate its intentions for taking photographs of students and will ask for consent before publishing them.
21.6 If the Trust wishes to use images/video footage of students in a publication, such as the Trust website, prospectus, or recordings of school plays, written consent will be sought for the particular usage from the parent of the student if the student is under 13 years of age, and from the student themselves otherwise.

22 Data retention

22.1 Data will not be kept for longer than is necessary, and always in accordance with the Trust's published retention schedule.
22.2 Data which is no longer required will be securely disposed of as soon as practicable.
22.3 Paper documents will be shredded or pulped, and electronic data securely deleted, once the data should no longer be retained.

23 Breach of the policy

23.1 Non-compliance with the requirements of this policy could lead to serious action being taken by third parties against the Trust. Non-compliance is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the Act, for example, by obtaining and disclosing personal data for their own purposes without the consent of the data controller.

24 Policy review

24.1 This policy is reviewed every two years by the Director of Operations and the Chief Executive Officer and approved by the Trust Board.