Bradford Diocesan Academies Trust

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

Issued: April 2018
Reviewed: March 2022
Next review: March 2024

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 have 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.

March 2020

10. Addition of biometric data (paragraph 22)
11. Update to CCTV (paragraph 21)
12. General update and minor revisions

March 2021

No substantive changes

March 2022

13. This policy has been updated to include information on GDPR Data Retention, the GDPR Privacy Notices for parents, carers, staff, and students, and GDPR Subject Access Request Guidance.

13. Information has been included which explains that certain safeguarding scenarios may be exempt from GDPR as directed by law and supported by government guidance (paragraph 2).

14. Appendix A Data Protection Impact Assessment added.

15. Appendix B has been added to show who holds which GDPR role within the Trust.

16. General update and minor revisions.

Bradford Diocesan Academies Trust

Contents Page

As part of our focus on diversity and inclusion, BDAT pledges that our policies will seek to promote equality, fairness, and respect for all staff and students. Our policies reflect the BDAT values of inclusion, compassion, aspiration, resilience, and excellence. By working closely with a range of stakeholders, such as our school, union, and HR colleagues, we have ensured that BDAT's policies do not unlawfully discriminate against anybody.

1. Introduction

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

1.2 This policy complies with our Funding Agreement and Articles of Association

2. Safeguarding and GDPR

It is important to note that the GDPR Act 2018 and the Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe. As stated in s27 of the government guidance 'Working Together to Safeguard Children' (July 2018), "Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children".

To effectively share information:

- All practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal.
- Where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent.
- Information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.
- Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

For further information on safeguarding and GDPR, please see the government guidance titled 'Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents, and carers' (July 2018).

3. Legal framework

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

- The General Data Protection Regulation (GDPR) 2018
- The Data Protection Act 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.
- The Protection of Freedoms Act 2012

3.2 This policy also has due 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'
- Information Commissioner's Office (2017) 'A data protection code of practice for surveillance cameras and personal information'
- HM Government (July 2018) 'Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents, and carers'
- HM Government (July 2018) 'Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children'

4. Applicable data

4.1 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.

4.2 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) 2018. 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.

5. Principles

5.1 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 it 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.

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

6. 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 are recorded using the Data Protection Impact Assessment which can be found in Appendix A.

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.

7. 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 Deputy Chief Financial Officer 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 suffer any detriment 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 for the academy for data protection issues. Staff will be made aware of who the person is.

6.8 Further detail on who holds what role within the Trust, definitions, and responsibilities can be found in Appendix B.

8. 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).

9. 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 2018 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 and carers 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.

10. 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 are available online on the Trust's policy page of the website.

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 as appropriate and relevant to the data and the data subject 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.

11. The right of access

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

11.2 Individuals have the right to submit a subject access request (SAR) to gain access to their Personal data. The Trust has a Subject Access Request Guide available on the policy page of the website.

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

11.4 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 actual 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 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.

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.

12. 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.

11.3 Where required, 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 may be extended by two months where the request for rectification is complex.

11.5 Where the Trust decides not to action for rectification, it 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.

13. 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 basis 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 up to 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 Trust data (where the Trust is the data controller). The use of a Trust or school implemented system is permitted. Dropbox is approved for use by the Education Teams for the storage and sharing of resources and non-sensitive data.

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/carers 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 individuals concerned.

20.4 When uploading information to the Trust website, staff are mindful of any deletions or subsequent 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. The ICO Code of Practice can be found here: code of practice

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.

21.7 The Trust CCTV Policy can be found on policy page of the website.

22 Biometric Recognition Systems

22.1 Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

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

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

22.4 Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners in cash at each transaction if they wish.

22.5 Parents/carers and students can withdraw consent, at any time, and the Trust will make sure that any relevant data already captured is deleted.

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

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

23 Breach of the policy

23.1 Non-compliance with the requirements of this policy could lead to legal action being taken by third parties against the Trust. Non-compliance may therefore be considered a disciplinary matter which. 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 year by the Deputy Chief Financial Officer and the Chief Executive Officer and recognised trade unions and approved by the Trust Board.

25 Data retention

BDAT recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust and academies therein. This document provides the policy framework through which this effective management can be achieved and audited.

25.1 Scope of this section on data retention

This section applies to all records created, received or maintained by staff in the Trust and academies in the course of carrying out their functions.

- Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
- A small percentage of records may be selected for permanent preservation as part of the institution's archives and for historical research.

25.2 Responsibilities

- The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The Chief Executive Officer has overall responsibility for this policy.
- The person responsible for records management in the Trust and academies will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.
- Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the Trust's records management guidelines.

25.3 Safe Disposal of Records

Where records have been identified for destruction they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information, should be shredded before disposal using a cross cut shredder. Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Employees should not put records in the dustbin or a skip.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction.

Members of staff should record at least:

- File reference (or other unique identifier).
- File title (or brief description) and number of files.
- The name of the authorising officer and the date action taken.

This should be kept in an Excel spreadsheet or similar suitable format.

25.4 Transfer of Information

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

25.5 Academy Closures

Should an academy close there will be records which will need to be stored until they work out their statutory retention periods.

It is the responsibility of the Trust to manage these records until they have reached the end of their administrative life and to arrange for their disposal when appropriate. There may be a number of different reasons why an academy has closed and this may affect where the records need to be stored.

- If the academy has been closed and the site is being sold or reallocated for another use then the Trust should take responsibility for the records from the date the school closes.
- If two academies have merged onto one site and then function as one academy, it is sensible to retain all the records relating to the two academies on the one site.

25.6 Retention Guidelines

The following retention guidelines have been issued by the Management Society of Great Britain 'Retention Guidelines for Schools'. Some of the retention periods are governed by statute. Others are guidelines following best practice.

Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation 2018 and the Freedom of Information Act 2000. Managing record series using these retention guidelines will be deemed to be 'normal processing' under the legislation mentioned above. If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

Please see Appendix C for an information retention and disposal checklist of archive periods.

26 Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.
The school is the 'data controller' for the purposes of data protection law.

Our data protection officer and contact details are below (see 'Contact us' below).

The personal data we hold
Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data
We use this data to:

- Support pupil learning
- Monitor and report on pupil progress

- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information
While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data
We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations.

Please refer to the Information and Records Management Society's toolkit for schools.

Data sharing
We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database
We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school and early years census if applicable.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.
For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Schools with pupils aged 13 and above

Youth support services
Once our pupils reach the age of 13, we are legally required to pass on certain information about them to [name of local authority or youth support services provider in your area], as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the relevant local authority or youth support service provider.

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

Parents/carers and pupils' rights regarding personal data

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

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents/carers also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the legally required information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Other rights
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously. If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents/carers and to reflect the way we use data in this school.

27 Privacy notice for staff

What is the purpose of this privacy notice?

BDAT is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the GDPR. It applies to all employees, workers and contractors.

BDAT is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice applies to current and former employees, workers and contractors. It does not form part of any contract of employment or other contract to provide services.

The categories of school workforce information that we collect, process, hold and share about you are:

- personal information (such as name, address, bank details, next of kin details, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as racial or ethnic origin, sexual orientation, religious beliefs, trade union membership, genetic or biometric data, medical information including health and sickness records and [information about criminal convictions and offences]
- contract information (such as start dates, hours worked, post, roles, training records and salary information)
- recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter as part of the application process)

- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- disciplinary, grievance and performance information
- CCTV footage and other information obtained through electronic means such as swipecard records
- information about your use of our information and communications systems
- photographs

How is your personal information collected?

We collect this information through the application and recruitment process, either directly from candidates or from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, your Church and other referees. We collect additional personal information in the course of job-related activities throughout the period during which you work for us.

Why we collect and use this information

We use school workforce information to:

- make decisions about recruitment, appointment, salary reviews, benefits and promotion
- check that individuals have the right to work in the UK
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid and, where appropriate, to deduct tax and National Insurance Contributions
- enable support for staff
- manage performance, training and development
- handle disciplinary, dismissal and grievance matters
- conduct restructuring and redundancy processes
- manage sickness absence
- ensure the health, safety and security of our workforce, both physically and on our computer systems
- monitor equal opportunities

The lawful basis on which we process this information

We need to process school workforce information for the following lawful reasons:

- to perform/administer the contract that we have entered into with you
- to comply with our legal obligations

We may also process school workforce information in the following situations, which are likely to be rare:

- where we need to protect your interests (or someone else's interests)

- where we need to do so in the public interest.

If you fail to provide personal information

If you fail to provide certain information when requested:

- we may not be able to deliver the contract that we have entered into with you (such as paying you or providing a benefit)
- we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workforce).

Change of purpose

We will only use school workforce information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Special categories of data

Information such as racial or ethnic origin, sexual orientation, religious beliefs, trade union membership, genetic or biometric data and medical information including health and sickness records requires higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- in limited circumstances, with your explicit written consent
- where we need to carry out our legal obligations or exercise rights in connection with your employment
- where it is needed in the public interest, such as for equal opportunities monitoring, gender reporting or for our occupational pension scheme
- less commonly, where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Information about criminal convictions

We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided that we do so in line with our data protection policy. Where appropriate, we will collect information about criminal convictions as part of the recruitment process, DBS checks or where we are notified of such information directly by you in the course of you working for us.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce information for the periods of time set out in our Data Retention Policy.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- the Education Skills Funding Agency (ESFA)
- Payroll provider
- HR provider
- Bank

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless we are required to do so by law, where it is necessary to administer the working relationship with you, or where we have another legitimate interest in doing so. We require third parties to respect the security of your data and to treat it in accordance with the law.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for

Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Rights of access, correction, erasure and restriction

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact your **Academy Data Protection Coordinator.** You will not usually have to pay a fee to access your personal information.

You also have the right to:

- object to processing of personal data where we are relying on a legitimate interest and the processing is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- request the transfer of your personal information to another party
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance by contacting BDAT's Data Protection Officer. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

28 Privacy notice for students

What is the purpose of this privacy notice?

BDAT is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your school career with us, in accordance with the GDPR. It applies to all students.

BDAT is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice applies to current and former students. It does not form part of any contract.

The categories of student information that we collect, hold and share about you are:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (progress, achievement)
- Relevant medical information
- Special Educational Needs information
- Behavioural Information
- Post 16 learning information

How is your personal information collected?

We typically collect information either directly or indirectly through application forms, examination entries, attendance records, medical records, attainment records, consent forms, computer records, photographs, video, CCTV and other applications.

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use student information to meet legal requirements and legitimate interests set out in the Education Act 1996 and Regulation 5 of the Education Regulations 2013. To conform with GDPR, any information the academy processes fulfils one of the following requirements from Article 6 of the GDPR:

- 1(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- 1(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- 1(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 1(e) 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.

Where we process special categories of personal data we do so under obligations covered in Article 9 of GDPR:

- 2(g) – the processing is necessary for reasons of substantial public interest.
- Where the above do not apply the academy will seek consent for specific purposes in line with the following Article 6.1.a.
- 1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

This will be done in writing and will clearly define any other uses of personal information and ask for consent for each and every use.

Change of purpose

We will only use student information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Special categories of data

This information includes ethnic group, medical information including health and sickness records and requires higher levels of protection. We will need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- in limited circumstances, with your explicit written consent
- where we need to carry out our legal obligations or exercise rights in connection with your

employment
- where is it needed in the public interest, such as for equal opportunities monitoring or for our occupational pension scheme
- less commonly, where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Information about criminal convictions

We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided that we do so in line with our data protection policy. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or where we are notified of such information directly by you in the course of you working for us.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

Where information forms part of a **student's** statutory education record, The Education Regulations 2005 SI 2005 No. 1437, the academy will retain the information for 25 years from the child's date of birth. Other information will be retained only where it is required to perform our legal obligations or where it is retained to safeguard and promote the welfare of children and in accordance with our Data Retention Policy.

Who we share student information with

We routinely share student information with:

- schools that the students attend after leaving us
- our local authority
- the Department for Education (DfE)
- School nursing service where appropriate
- NHS where appropriate

Why we share student information

We do not share information about our students with anyone without consent unless we are required to do so by law, or where we have another legitimate interest in doing so. We require third parties to respect the security of your data and to treat it in accordance with the law.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit the local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in

electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Rights of access, correction, erasure and restriction. Under data protection legislation, parents, carers, and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact **the Data Protection Coordinator at the academy at which your child is registered.** You will not usually have to pay a fee to access your personal information.

You also have the right to:

- object to processing of personal data where we are relying on a legitimate interest and the processing is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- request the transfer of your personal information to another party
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

29 Subject Access Request Guidance

GDPR provides individuals the right of subject access to information about themselves. It does not give a right of access to information about anyone else - unless it is a parent acting on behalf of a child, for example. The Trust GDPR Policy can be found on the website.

It is important that the Data Controller ensures that third party information is removed from the record prior to release to the applicant (data subject) unless the third party has given their consent to the release of the information.

What is a subject access request?

The legislation ensures transparency of processing personal data by obliging data controllers to explain to individuals how their data will be processed and the right of data subjects to access that information.

A data subject may make a formal request to any organisation to have a copy of all data in which that person may be identified. There is a need for transparency of processing to ensure that individuals can identify those organisations which have access to and process their data. This enables them to understand how their personal information is to be used and to exercise their rights over the processing of that information.

The importance of the right of subject access in Data Protection law cannot be overestimated; it is often only by exercising the right to see their information that individuals can determine whether other breaches of legislation have occurred. Data subjects are often interested in documentation which may be about them, but they have not seen.

Because of the importance of the subject access rights, complaints about an organisation's failure to comply with a request for subject access are taken very seriously by the ICO. Such complaints are dealt with as a matter of priority and may often lead to a full-scale investigation into an organisation's procedures and practices.

What is a valid subject access request?

A request must be in writing although reasonable adjustments should be made if a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing. A request sent by e-mail or fax is as valid as one sent in hard copy.

It must request access to their personal information (held either manually or electronically) and not to information relating to other people.

If a request does not mention the GDPR specifically or even say that it is a subject access request, it is still valid and should be treated as such if it is clear that the individual is asking for their own personal data.

It may be restricted to only limited information (but need not be).

It must be made by the data subject (or by a person authorised by or with responsibility for the data subject). The Trust and all of its academies will take reasonable steps to verify that the person making the subject access request is the data subject (e.g. ID verification check).

A copy of the information held on a data subject must be provided free of charge, however the Trust withholds the right to charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if repetitive.

The Trust may also charge reasonable additional fees for further copies of the same information. This does not mean however that the Trust can charge for subsequent access requests.

A SAR must be complied with within one month from the date of receipt of the request. The Trust holds the right to extend the period of compliance up to a further two months, where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Primary schools:

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Secondary schools:

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of

the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Finding and Checking the Requested Information

If an employee receives a subject access request for information it is important that they do not respond to the query direct, but instead liaise immediately, with the Data Protection Coordinator who will manage the agreed process within the one-month window:

- Check the validity of the request and if necessary will send the request form for completion and/or validation of information request and/or request for fee
- Log details and acknowledge receipt of the request and fee
- Pass details to Data Protection Coordinator so they can contact the relevant Manager to provide all data each department is holding on the individual and confirms response date.
- Each relevant department checks records. These include manual records, system information, audiotapes and archive data (if required) and CCTV data (if required) – please see CCTV Policy on the website.
- Once each relevant department responded by forwarding the relevant data to the Data Protection
  Officer, the data will be checked in line with this policy. All the requested information should be printed out or photocopied and will be sent to the individual with a covering letter by special delivery and/or email

Denial of Access

The Trust may refuse a subject access request when a request is manifestly unfounded or excessive, or deemed to be particularly repetitive.

If the Trust refuses to respond to a request, it must explain why to the individual, informing them of their right to complain to the supervisory authority (Information Commissioners Office) and to a judicial remedy without undue delay and at the latest within one month of receipt of the request.

Exemptions

The Trust has to protect the legal rights of other individuals when responding to a subject access request including trade secrets or intellectual property. The consideration of exemptions should not be a refusal to provide all information to a data subject. Where the data controller processes a large amount of data regarding the subject, it is reasonable to request that the subject specify the information and processing activities to which the request relates.

Bradford Diocesan Academies Trust

Appendix A – Data Protection Impact Assessment

DATA PROTECTION IMPACT ASSESSMENT

Category	Information
Date of assessment	
Who did the assessment?	
The name of the Data Protection Officer	
Name of process	
Purpose of process	
Under what legal basis are you processing the information?	
Where does the data come from?	
In which locations does the processing take place?	
Who is impacted by the processing?	
What is the process for deleting the data?	
Describe the process workflow	
Links to related documents	
What are the risks to the data subjects	
What measures are currently in place to protect the data subject and their rights?	
What additional measures will you put in place to ensure all risks are covered?	
Data of next review	

Bradford Diocesan Academies Trust

Appendix B – GDPR roles within the Trust

Title	Definition	Who holds this position	Further information
Data Controller	The person, or company, who determines the purposes for which, and the way in which, personal data is processed.	The Trust	The Data Controller must ensure processing, including any processing carried out by a processor on behalf of the Trust, complies with GDPR. Duties include collecting the individual's consent, storing of the data, managing consent-revoking, enabling the right to access, and more.
Data Processor	The data processor is responsible for processing personal data on behalf of the data controller.	Employees	A number of Trust employees will work with personal data as part of their day to day role. These employees will receive appropriate GDPR training.
Data Subjects	The identified or identifiable living individual to whom personal data relates.	A variety of people associated with the Trust fall under this category e.g. employees, job applicants, volunteers (including governors), contractors, etc.	It is necessary to hold personal data as part of the day to day operations of the Trust e.g. when applying for a job within the Trust, applicants must provide a number of personal details such as their name and address. All personal data will be stored in accordance with the Data Retention Policy.
Data Protection Officer (DPO)	Informs and advises the Trust and its employees about their obligations to comply with GDPR and data protection laws.	Deputy CFO	The DPO must monitor the Trust's compliance with 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.
Data Protection Coordinator (DPC)	An academy employee who is the central point of contact for the academy for data protection issues.	Academy employee – usually the SBM	Academy staff will be aware of who this person is, and can approach this person in the first instance for all GDPR related queries. The DPC will liaise with the DPO regularly e.g. to report breaches, seek advice, etc.

Bradford Diocesan Academies Trust

Appendix C - Information Retention and Disposal Checklist of Archive Periods

Finance and Procurement

Description	Record	Retention Period	Action	Citation
Financial Management	Records documenting the development and establishment of the Finance Strategy.	Superseded + 10 years	Review or Archive Value	n/a
	Records documenting the monitoring of performance against the organisation KPIs - core data	Current financial year + 1 year	Destroy	n/a
	Records documenting the monitoring of performance against the organisation KPIs - reports	Current financial year + 10 years Last action on audit + 6 years	Review or Archive Value	n/a
Financial Audit	Records documenting the conduct and results of financial audits, and action taken to address	Current financial year + 6 years	Destroy	1980 c.58
Financial Accounting	Records documenting the issue of sales invoices and the processing of incoming payments	Current financial year + 6 years	Destroy	1970 c.9 1980 c.58 1994 c.23
	Records documenting the receipt and payment of purchase invoices	Current financial year + 6 years	Destroy	1970 c.9 1980 c.58 1994 c.23
	Records of the handling of petty cash	Current financial year + 6 years	Destroy	1970 c.9 1980 c.58 1994 c.23
	Records of the receipt and processing of students' fees	Current financial year + 6 years	Destroy	1970 c.9 1980 c.58

Description	Record	Retention Period	Action	Citation
	Records documenting the preparation of the organisations statutory accounts	Current financial year + 6 years	Destroy	1980 c.58
	Annual accounts	Closure of account + 6 years	Archive	1970 c.9

Description	Record	Retention Period	Action	Citation
Financial Accounting	Records of opening, closing and routine administering of bank accounts	Current financial year + 6 years	Destroy	1980 c.58
	Records of standing order, direct debits	Life of instruction + 6 years	Destroy	1980 c.58
	Records of routine bank account deposits/ withdrawals/transfers (paying-in slips, transfer instructions, bank statements etc.)	Current financial year + 6 years	Destroy	1980 c.58 1970 c.9
	Records of the processing of internal accounting transactions between operating unitys (i.e. cross-charges)	Current financial year + 1 year	Destroy	n/a
Management Accounting	Records documenting analyses of the internal deployment of the organisation's financial resources	Current financial year +1 year	Destroy	n/a
	Management Account Journals	Current financial year + 6 years	Destroy	n/a
	Financial systems documentation	Life of system	Destroy	n/a
	Financial Statement	Permanently	n/a	n/a

Description	Record	Retention Period	Action	Citation
Budget management	Preparation of annual operating budgets	Current financial year + 1 year	Destroy	n/a
	Monitoring of income and expenditure against annual operating budgets, and action take to deal with variances	Current financial year + 1 year	Destroy	n/a
Funding administration	Administering annual funding allocations from appropriate statutory funding bodies (inc correspondence, invoices)	Current financial year + 10 years	Destroy	n/a

Description	Record	Retention Period	Action	Citation
Payroll Administration	Calculation and payment of payroll payments to employees	Current tax year + 6 years	Destroy	1970 c.9 1980 c.58 1993/774 1999/584
	Employees' authorisation for non-statutory payroll deductions e.g. gym membership, nursery vouchers, travel loans, etc	Current tax year + 6 years	Destroy	1980 c.587
	Records documenting the operation of the statutory sick pay scheme	Current tax year + 3 years	Destroy	1982/894
	Records documenting the operations of statutory maternity scheme	Current tax year + 3 years	Destroy	1986/1960
	Records documenting the payment and/or reimbursement of employees' and Board members' expenses	Current financial year + 6 years Current financial year + 2 years	Destroy	1970 c.9 1980 c.58
	Payroll reconciliation	Termination of employment + 75 years	Destroy	

Description	Record	Retention Period	Action	Citation
Pension Administration	Records documenting payments of the organisation's employer's contributions to pensions schemes for its employees	Termination of employment + 75 years	Destroy	1980 c.58
	Records of payment of employee's contribution to pension schemes	Current tax year + 6 years	Destroy	1980 c.58
Tax Management	Records documenting the preparation and filing of the organisation's tax returns	Current tax year + 6 years	Destroy	1994 c.23
	Assessment of tax liabilities	Current tax year + 6 years	Destroy	1994 c.23
	VAT account	Current tax year + 3 years	Destroy	1994 c.23
	PAYE/NI/returns on subcontractors	Commencement of policy + 40 years	Destroy	1970 c.9

Description	Record	Retention Period	Action	Citation
Insurance Management Policy	Records documenting the arrangement and renewal of insurance policies to meet defined requirements and legal obligations: Employers' Liability insurance (organisations has exemption certificate)	Commencement of policy + 40 years OR Renewal of policy + 40 years	Destroy	1980 c.58
	Records documenting the arrangement and renewal of insurance policies to meet defined requirements and legal obligations: all other insurance	Expiry of policy + 6 years	Destroy	1980 c.58

Description	Record	Retention Period	Action	Citation
	Records documenting claims made under insurance policies: property and other claims	Settlement of claim + 6 years OR Withdrawal of claim + 6 years	Destroy	1980 c.58
	Records documenting claims made under insurance policies: liability/personal injury/nurture claims	Permanent	N/A	1980 c.58
Asset Management	Valuation of capital assets	Current financial year + 6 years	Review for Archive	1970 c.9
	Records documenting the disposal of capital assets	Disposal financial year + 6 years	Review for Archive	1970 c.9 1980 c.58
Supplier approval	Records documenting supplier evaluation criteria	Superseded + 5 years	Destroy	n/a
	Records documenting invitation to prospective suppliers to apply for approval	Expiry of invitation OR Rejection of application + 6 months completion of approval	Destroy	n/a
	Records documenting the evaluation of applications for approval for prospective suppliers, and notification of the outcome: approved suppliers.	Termination of approval	Destroy	n/a

Description	Record	Retention Period	Action	Citation
Supplier approval	Records documenting the evaluation of applications for approval from prospective suppliers, an notification of the outcome: rejected	Rejection + 1 year	Destroy	n/a

Description	Record	Retention Period	Action	Citation
	suppliers			
	Supplier database	While current	Destroy	n/a
Supply contract tendering	Records documenting the process of inviting and evaluating pre-qualification submissions from prospective suppliers	Award of supply contract + 1 year	Destroy	191/2680 1993/3228 1995/201
	Records documenting invitation to tender and tender evaluation criteria	Termination of supply contract awarded + 6 years	Destroy	1980 c.58 1991/2680 1993/3228 1995/201
	Records documenting the issues of Invitation to Tender and handling of incoming tenders	Award of supply contract + 1 year	Destroy	1991/2680 1993/3228 1995/201
	Records documenting the evaluation of tenders, the conduct of negotiations with tenders and the notification of the results of the tender evaluation process: rejected tenders	Award of supply contract + 1 year	Destroy	1991/2680 1993/3228 1995/201
	Records documenting the evaluation of tenders the conduct of negotiations with tenders and the notification of the results of the tender evaluation process: accepted tenders	Termination of supply contract awarded + 6 years	Destroy	1980 c.58 1991/2680 1993/3228 1995/201
	Contract aware report (as required by the regulations cited)	Termination of supply contract awarded + 6 years	Destroy	1980 c.58 1991/2680 1993/3228 1995/201

Description	Record	Retention Period	Action	Citation
	Statistical reports on contracts awarded (as required by external financial regulations)	Date of creation + 3 years	Destroy	1980 c.58 1991/2680 1993/3228 1995/201

Description	Record	Retention Period	Action	Citation
Supply contract management	Records documenting variations to contracts (e.g. revisions, extensions)	Termination of contract + 6 years	Destroy	1980 c.58
	Records documenting the monitoring of supplier performance and action taken regarding under-performance	Termination of contract + 6 years	Destroy	1980 c.58
Purchasing administration	Records documenting purchasing authorisation limits.	Superseded + 1 year	Destroy	n/a
	Records document internal authorisation for procurement.	Current financial year + 1 year	Destroy	n/a
Strategy, policies and procedures	HR Strategy: Master copy	Permanent	Retain	
	HR Strategy: Working papers	Adoption + 2 years	Destroy	n/a
	HR Policies	Superseded + 5 years	Destroy	n/a
	HR Policies: Working papers	Adoption + 2 years	Destroy	n/a
	HR Procedures and guidance	Adoption + 2 years	Destroy	n/a

Description	Record	Retention Period	Action	Citation
	HR Procedures and Guidance working papers	Adoption + 2 years	Destroy	n/a
Workforce Planning	Assessment and analysis of workforce requirements and the identification and evaluation of options for meeting requirements	Creation + 5 years	Review	1980 c.58 s.2
	Records documenting management succession or restructuring plans	Superseded + 5 years	Review	n/a
	Records documenting the internal analysis and discussion for the creation of a new post	Creation + 3 years	Destroy	n/a

Description	Record	Retention Period	Action	Citation
Workforce Planning	Job evaluation exercises: working papers	Completion + 1 year	Destroy	n/a
	Job evaluation exercises: results	Completion + 10 years	Destroy	n/a
Recruitment	Individual job description and personal specification	Termination + 6 years	Destroy	n/a
	Grading of individual jobs: outcomes	Superseded + 10 years	Destroy	n/a
	Grading of individual jobs: correspondence and working papers	Upon advertisement of post	Destroy	n/a
	Authorisation to recruit	Completion of appointment + 5 years	Destroy	n/a

Description	Record	Retention Period	Action	Citation
	Advertisement of vacancies; working papers	Appointment of successful candidate + 6 months	Destroy	1975 c.65 1976 c.74 1995 c.50
	Advertisement text (screenshot)	Termination of employment in role	Destroy	n/a
	Enquiries about vacancies and requests for application forms	Completion of appointment + 6 months	Destroy	n/a
	Review/short listing of applicants	Completion of appointment + 5 years	Destroy	n/a
	Selection of staff: interview notes, test results (successful and unsuccessful candidates)	Completion of appointment + 6 years	Destroy	n/a
	Application forms (excluding equal opportunities monitoring form) and CVs: successful candidates	Retain for 6 years after termination of employment.	Destroy	1980 c.58 s.2

Description	Record	Retention Period	Action	Citation
Recruitment	Application forms and CVs: unsuccessful candidates	Completion of appointment + 6 months	Destroy	n/a
	References successful candidates	Provision of references + 6 months	Destroy	n/a
	References unsuccessful candidates	Completion of appointment + 6 months	Destroy	n/a
	Recommendation to recruit individual	Completion of appointment + 5 years	Destroy	n/a

Description	Record	Retention Period	Action	Citation
	DBS clearance documentation	Date of clearance + up to a maximum of 6 months	Destroy	DBS code of practice
	Clearance to work documentation	Retain for 6 years after termination of employment	Destroy	n/a
	Equal opportunities form	Immediately after information entered onto database	Destroy	n/a
	Equal opportunities database information	Entry + 10 years	Destroy	n/a
	Equal opportunities regular statistical reports	Creation + 10 years	Destroy	n/a
	Equal opportunities ad hoc statistical reports	Creation + 2 years	Destroy	n/a
	Data for analyses of recruitment effectiveness	Analyses + 6 months	Destroy	n/a
	Analyses of recruitment effectiveness	Analyses + 3 years	Destroy	n/a
	Unsolicited applications	Reply + 6 months	Destroy	n/a

Description	Record	Retention Period	Action	Citation
Training, development, induction and performance	Identification of staff development needs and the development of plans to meet those needs	Creation + 5 years	Review	1980 c.58 s.2

	Records documenting the development, overall delivery and assessment of induction or other training programme	Current year + 2 years	Destroy	n/a
	Feedback analysis of induction or other training programmes.	Current year + 2 years	Destroy	n/a
	Records documenting the administration of induction or other training sessions, including feedback forms	Current year + 1 year	Destroy	n/a
	Records documenting analyses of the impact of training and development programmes	Current year + 4 years	Destroy	n/a
	Probation review/reports	Current year + 2 years	Destroy	n/a
	Annual appraisal documents	Current year + 5 years	Destroy	n/a
	Quarterly appraisal documents	Current year + 2 years	Destroy	n/a
Remuneration and reward	Records documenting the development of the organisation's remuneration structure and strategy	Superseded + 6 years	Review	n/a
	Records documenting pay reviews	Creation + 6 years	Review	n/a
	Records documenting reward and progression schemes	Creation + 6 years	Review	1980 c.58 s.2
	Records documenting individuals wage/salary records	Creation + 6 years	Review	1980 c.58 s.2

Description	Record	Retention Period	Action	Citation
Workforce Relations	Grievances: record of investigations where allegation are unsubstantiated	Conclusion of investigation + 6 months (a note may be retained showing the investigation too place but allegation was unsubstantiated)	Destroy	n/a
	Grievances: record of investigation and outcomes	Last action of investigation + 6 years	Destroy	1980 c.58 s.2
	Disciplinary: record of investigation where allegation are unsubstantiated	Conclusion of investigation + 6 months (a note may be retained showing investigation took place but allegation was unsubstantiated)	Destroy	n/a
	Disciplinary: Oral warnings	Date of issue + 1 year	Destroy	1980 c.58 s.2
	Disciplinary: written and other formal warnings	Retain for period stipulated when issued (usually date of issue + 1 year)	Destroy	1980 c.58 s.2
	Equality complaints handling (Human Resources related)	Last action of investigation + 6 years	Destroy	1980 c.58 s.2
	Workforce surveys and consultations	Completion of survey + 5 years	Review	n/a
	Workforce – individual responses to surveys	Completion of analysis	Destroy	n/a
	Workforce – summary of survey results	Completion of survey + 5 years	Review	n/a

	Performance assessment development	Life of assessment + 5 years	Review	n/a
	Summary results of performance assessments (anonymous)	Current year + 3 years	Review	n/a

Description	Record	Retention Period	Action	Citation
Workforce Relations	Analysis of impact of performance assessments	Current year + 3 years	Review	n/a
Employee welfare	Development of welfare schemes and services	Current year + 3 years	Review	n/a
	Monitoring of hours worked	Date of record + 2 years	Destroy	S.I 1998/1833
	Referrals to Occupational Health provider by self or manager	Last treatment + 10 years	Destroy	n/a
Industrial relations	Recognition of union	(De)recognition + 6 years	Review	1980 c.58 s.2
	Agreements with unions	End of agreement + 10 years	Review	1980 c.58 s.2
	Routine communication including minutes of meetings	Current year + 20 years	Review	n/a
	Consultation and negotiations	Last action + 20 years	Review	n/a
Employee contract management	Contract of employment	Termination of employment + 6 years	Destroy	n/a

	Changes to terms and conditions	Termination of employment + 6 years	Destroy	n/a
	Records of termination of employment by resignation, redundancy (inc estimates), retirement, dismissal (excluding compromise agreements)	Termination of employment + 6 years	Destroy	1980 c.58 s.5
	Individual staff: statutory leave entitlement e.g. parental leave	Completion of entitlement + 6 years	Destroy	SI 1999/3312
	Income tax and National Insurance correspondence with HMRC	Termination of employment + 6 years	Destroy	n/a
	Statutory sick pay and statutory maternity pay	Current tax year + 3 years	Destroy	n/a
Description	**Record**	**Retention Period**	**Action**	**Citation**
Employee contract management	Major injuries arising from workplace accidents, exposure to hazardous substances, disease	Termination of employment + 40 years	Destroy	n/a
	Compromise agreements and agreed forms of reference	Termination of employment + 40 years	Destroy	n/a
	Ex-staff records: pension files	Termination of employment + 75 years	Destroy	n/a
Pensions	Records documenting the organisation's relationships with pension schemes	End of relationship + 5 years	Destroy	1980 c.58 s.2
	Routine communications with the pension schemes	Creation + 5 years	Destroy	1980 c.58 s.2
	Individual staff pension information (inc opt in/out form)	Termination of employment + 6 years	Destroy	1980 c.58 s.2

	Records in relation to ex-staff now pensioners	Cessation of benefits + 12 years	Destroy	n/a
Management information	Senior HR team minutes and papers master set	Permanent	Retain	n/a
	Staff committee minutes and papers: master set	Permanent	Retain	n/a
	Statistics on staff turnover	Creation + 5 years	Destroy	n/a
	Benchmarking results for short term contracts	Creation + 10 years	Destroy	n/a
Contracts and agreements	Records documenting the negotiation, establishment and review of contracts and agreements between the organisation and third parties: agreements and contracts under seal (by deed)	Termination of contract + 12 years	Destroy	1980 c.58 s.8
	Records documenting the negotiation, establishment and review of contracts and agreements between the organisation and third parties: other contracts and agreements	Termination of contract + 6 years	Destroy	1980 c.58 s.8
Description	**Record**	**Retention Period**	**Action**	**Citation**
Legal Claims	Records documenting the provision of legal support and representation for the organisation in dealing with claims by or against the organisation which do not proceed to litigation or settlement by an agreement	Settlement of claim + 6 years OR Withdrawal of claim + 6 years	Destroy	1980 c.58 s.8
	Records documenting litigation between the organisation and third parties where legal precedents are set	Life of organisation	Permanent	n/a

	Records documenting litigation between the organisation and third parties which does not set legal precedents	Settlement of case + 6 year	Destroy	1980 c.58 s.2 and s.5
Legal interpretation and advice (records documenting legal advice requested by, and provided to, the organisation, concerning)	Interpretation of legislation affecting the organisation's legal framework, governance, responsibilities or operations	Life of organisation	Permanent	n/a
	Proposals for new legislation affective the organisation's legal framework, governance, responsibilities or operations	Life of organisation	Permanent	n/a
	The organisation's relationships with government bodies and regulators	Life of organisation	Permanent	n/a
	Industrial relations issues	Life of organisation	Permanent	n/a
	Health, safety and environmental issues	Life of organisation	Permanent	n/a
	Records documenting legal advice on other matters requested by, and provided to, the organisation	Superseded + 5 years	Destroy	n/a
Property acquisition	Records documenting the acquisition of ownership of properties	Ownership of property	Destroy	n/a
	Deeds and certificates of title for properties owned by the institution	Ownership of property	Destroy	n/a

Description	Record	Retention Period	Action	Citation
Property acquisition	Records documenting negotiations for properties where the property was not acquired	Closure of negotiations + 6 years	Destroy	1980 c.58
	Records documenting the acquisition of use of properties by lease or rental	Disposal of property + 6 years	Destroy	1980 c.58
Property Disposal	Records documenting the disposal of properties	Disposal of property + 6 years	Destroy	1980 c.58
Legal Framework	Records documenting the establishment and development of the organisation's legal framework	Life of organisations	Permanent	n/a
Governing body/ Board Management Governing body/ Board Management	Records documenting the appointment of members of the governing body/board. This information will be retained by the Legal Services Board	Termination of appointment + 6 years	Destroy	1980 c.58 s.5
	Records documenting the provision of training and development for members of the governing body//board. This information will be retained by the Legal Services Board.	Date of creation + 3 years	Destroy	n/a
	Records documenting the arrangements of meetings of the governing body/Board.	Date of creation + 1 year	Destroy	n/a
	Records documenting the conduct and proceeding of meetings of the governing body/board, agenda, minutes and supporting papers.	Date of creation + 50 years	Review	n/a
Board committee administration	Records documenting the development and establishment of terms of reference for committees.	Life of organisation	Permanent	n/a

	Records documenting the appointment of members of the committees.	Termination of appointment + 6 years	Destroy	1980 c.58 s.5
	Records documenting the provision of training and development committee members.	Termination of appointment + 6 years	Destroy	n/a

Description	Record	Retention Period	Action	Citation
Board committee administration	Records documenting training undertaken by individual member of a committee	Termination of appointment + 6 years	Destroy	1980 c.58 s.2 and s.5
	Records documenting the arrangements for meetings of a committee.	Current year + 1 year	Destroy	n/a
	Records documenting the organisations of meetings of Board Committees	Date of creation + 1 year	Destroy	n/a
	Records documenting the conduct and proceedings of meetings of Board committees, agenda, minutes and supporting papers	Date of creation + 50 years	Review	n/a
Organisation committee administration	Records documenting the development and establishment of the terms of reference, and the rules and procedures, for a committee	Life of committee + 6 years	Destroy	1980 c.58 s.5
	Records documenting the appointment / election / designation of members of a committee	Termination of membership + 6 years	Destroy	1980 c.58 s.5
	Records documenting the arrangements for meetings of a committee	Current year + 1 year	Destroy	n/a

	Records documenting the conduct of the business of a committee: agenda, minutes and supporting papers	Life of committee + 5 years	Destroy	n/a
	Records documenting the conduct of the business of a committee: correspondence and other records relating to the preparation of committee business or to actions to be taken (or not taken) as a result of committee decisions.	Current year + 5 years	Destroy	n/a
	Records documenting the appointment/election/designation of the organisation's senior officers	Termination of appointment + 6 years	Destroy	1980 c.58 s.5

Description	Record	Retention Period	Action	Citation
Public interest disclosure (whistleblowing) investigation	Records documenting the investigation, determination and resolution of an allegation made by a member of staff under the public interest disclosure act 1998	Closure of case + 6 years	Destroy	1980 c.58 s.2 and s.5
Official external representation (the activities involved in representing the organisation officially on external bodies)	Records documenting the appointment/designation of staff to officially represent the organisation	Termination of representation	Destroy	n/a
Risk Management identification and assessment	Records documenting identified risks to the organisation and assessments of those risks	Superseded + 1 year	Destroy	n/a

Business continuity planning	Records documenting identified risks to the organisation and assessments of those risks	Superseded + 1 year	Destroy	n/a
Internal and external audit management	Records documenting the planning of audits	Completion of Audit + 5 years	Destroy	n/a
	Records documenting the conduct of audits	Completion of Audit + 5 years	Destroy	n/a
	Records documenting the results of audits	Life of organisation	Permanent	n/a
	Records reviewing and responding to audit reports, including drawing up action plans to address issues raised	Life of organisation	Permanent	n/a
Organisation strategy development	Records documenting the development and establishment of strategy	Superseded + 10 years	Review	n/a
Organisation business planning	Records documenting the formulation of plans for implementing strategy	Superseded + 3 years	Review	n/a

Description	**Record**	**Retention Period**	**Action**	**Citation**
Organisation policy and procedural development	Policy development working papers	Superseded + 2 years	Review	n/a
	Approved policy	Superseded + 10 years	Review	n/a
	Procedure development working papers	Superseded + 1 year	Review	n/a
	Approved procedure	Superseded + 5 years	Review	n/a

Case management	Complaint case file including case call recording	Closure/last contact + 1 year	Destroy	n/a
	Non-case call recording	Closure/last contact + 1 year	Destroy	n/a
Internal complaints	Complaints case file including case call recording	Closure/last contact + 1 year	Destroy	n/a
	Non-case call recording	Closure/last contact + 1 year	Destroy	n/a
Subject access requests (Data Protection Act)	Request for information	Closure/last contact + 1 year	Destroy	n/a
Freedom of information requests	n/a	n/a	n/a	n/a
Environmental information requests	n/a	n/a	n/a	n/a
Performance Management	Performance monitoring reports	Current year + 3 years	Review	n/a
	Performance monitoring data and analysis	Current year + 3 years	Review	n/a
	Audit reviews, results and responses	Current year + 3 years	Review	n/a

Description	Record	Retention Period	Action	Citation
Quality Standards Management	Annual performance monitoring	Current year + 3 years	Review	n/a
	Internal reviews and audit	Current year + 3 years	Review	n/a

	Customer feedback: data and analysis	Current year + 3 years	Review	n/a
	Customer feedback: reports	Current year + 3 years	Review	n/a
	Development of the organisation's internal quality assurance processes.	Current year + 3 years	Review	n/a
	Conduct and results of internal and external review of research quality, and responses to the results	Current year + 3 years	Review	n/a
Research and enterprise	Records of the development, establishment and implementation of the organisation's research strategy	Superseded + 10 years	Review	n/a
	Records of strategy review (includes all data, reports and audit material)	Current year + 10 years	Destroy	n/a
	Announcements of research resulting in publication or through the media	Issue of announcement + 3 years	Destroy	n/a
	Preparation of publications, presentations, demonstrations or other means of disseminating research results.	Publication / delivery + 3 years	Destroy	n/a
Project Management	Records documenting the management of internally-funded research projects (e.g. budgets staff etc.)	Completion of project + 3 years	Destroy	n/a
	Records documenting the management of externally-funded research projects (e.g. budgets, staff etc.)	Completion of project + 6 years (unless a longer period is required by sponsor contract)	Destroy	1980 c.58

Bradford Diocesan Academies Trust

Retention schedule citations

Acts of the UK Parliament	**Statutory instruments of the UK parliament**
1957 c.31 Occupiers Liability Act 1957 1969 c.57 Employers' Liability (Compulsory Insurance) Act 1969 1970 c.9 Taxes Management Act 1970 1970 c.41 Equal Pay Act 1970 1974 c.37 Health and Safety at Work etc. Act 1974 1975 c.65 Sex Discrimination Act 1975 1976 c.74 Race Relations Act 1976 1980 c.58 Limitation Act 1980 1992 c.4 Social Security Contributions and Benefits Act 1992 1994 c.23 Value Added Tax Act 1994 1994 c.30 Education Act 1994 1995 c.50 Disability Discrimination Act 1995 1998 c.29 Data Protection Act 1998	S.I. 1977 / 500 The Safety Representatives and Safety Committees Regulations 1977 S.I. 1981 / 917 The Health and Safety (First Aid) Regulations 1981 S.I. 1982 / 894 The Statutory Sick Pay (General) Regulations 1982 S.I. 1986 / 1960 The Statutory Maternity Pay (General) Regulations 1986 S.I. 1989 / 635 The Electricity at Work Regulations 1989 S.I. 1989 / 682 The Health and Safety Information for Employees Regulations 1989 S.I. 1989 / 1790 The Noise at Work Regulations 1989 S.I. 1991 / 2680 The Public Works Contracts Regulations 1991 S.I. 1992 / 2792 The Health and Safety (Display Screen Equipment) Regulations 1992 S.I. 1992 / 2793 The Manual Handling Operations Regulations 1992 S.I. 1992 / 2932 The Provision and Use of Work Equipment Regulations 1992 S.I. 1992 / 2966 The Personal Protective Equipment at Work Regulations 1992 S.I. 1993 / 744 The Income Tax (Employments) Regulations 1993 S.I. 1993 / 3228 The Public Services Contracts Regulations 1993 S.I. 1995 / 201 The Public Supply Contracts Regulations 1995 S.I. 1995 / 3163 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 S.I. 1996 / 341 The Health and Safety (Safety Signs and Signals) Regulations 1996 S.I. 1996 / 972 The Special Waste Regulations 1996 S.I. 1996 / 1513 The Health and Safety (Consultation with Employees) Regulations 1996 S.I. 1997 / 1840 The Fire Precautions (Workplace) Regulations 1997 S.I. 1998 / 1833 The Working Time Regulations 1998 S.I. 1998 / 2306 The Provision and Use of Work Equipment Regulations 1998 S.I. 1998 / 2307 The Lifting Operations and Lifting Equipment Regulations 1998 S.I. 1998 / 2573 The Employers' Liability (Compulsory Insurance) Regulations 1998 S.I. 1999 / 584 The National Minimum Wage Regulations 1998 S.I. 1999 / 3242 The Management of Health and Safety at Work Regulations 1999 S.I. 1999 / 3312 The Maternity and Parental Leave etc. Regulations 1999

	S.I. 2002 / 2675 The Control of Asbestos at Work Regulations 2002 S.I. 2002 / 2676 The Control of Lead at Work Regulations 2002 S.I. 2002 / 2677 The Control of Substances Hazardous to Health Regulations 2002
Other provisions HMCE 700/21 HM Customs and Excise Notice 700/21: Keeping [VAT] records and accounts IR CA30 Statutory Sick Pay Manual for employers CA30	