Bradford Diocesan Academies Trust

UK General Data Protection Regulation Policy (UK G.D.P.R.)

Reviewed: June 2025

Review: June 2027

Bradford Diocesan Academies Trust

Table of Contents

1.0 Policy Statement

BDAT is required to keep and process certain information about its staff and students in accordance with its legal obligations under the UK General Data Protection Regulation (UKGDPR).

This policy is in place to ensure the Trust Board and all Trust staff are aware of their responsibilities and it outlines how the Trust and Trust academies comply with the following core principles of the UK GDPR.

2.0 Scope and Purpose

2.1 Legal framework

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

• The UK General Data Protection Regulation (UKGDPR)

• The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy will also have regard to guidance produced by the Information Commissioner's Office (ICO).

This policy will be implemented in conjunction with the following Trust policies and procedures;

- BDAT CCTV Policy
- BDAT Social Media Policy
- BDAT Child Protection and Safeguarding Policy
- BDAT Data Retention Schedule Protocol
- BDAT Data Protection Impact Assessments (DPIA) Procedure
- BDAT Data Breach Management Procedure
- BDAT Data Subject Access Request Procedure
- BDAT Freedom of Information Act Policy

2.2 Controller and Processor

BDAT and BDAT academies are both a "Controller" and "Processor" of personal data. BDAT IS registered as a "Controller" with the Information Commissioner's Office:

- A "Controller" determines the purpose and means of processing personal data
- A data "Processor" processes personal data on behalf of the data controller.

2.3 Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual e.g. employee, job applicant, student, parent/carer, volunteer, contractor,

freelancer, board member. The UKGDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria:-

• **Personal data** includes information such as name, address, date of birth, National Insurance Number; email address (personal and business), chronologically ordered data and pseudonymised data e.g. Unique Pupil Numbers, Admission Numbers, Employee Numbers, key-coded data and online identifiers, e.g. IP addresses.

• **Sensitive personal data** is referred to in the UKGDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union membership, genetic data, biometric data, health, sex life and sexual orientation. In schools this could also be staff sickness absence, diversity monitoring, photos etc. There are strict rules surrounding the processing of special categories of personal data.

3.0 Overarching Principles

In accordance with the requirements outlined in the UKGDPR, personal data must be:-

- Processed lawfully
- For a specific purpose
- Kept to a minimum
- Accurate and up-to-date
- Retained only for as long as it is needed
- Kept securely

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

4.0 Responsibilities and Arrangements

4.1 Accountability

BDAT, as a publicly funded organisation, has to appoint a Data Protection Officer (DPO), this is the **Deputy CFO**. Their duties will include:

• Informing and advising the Trust and staff about their obligations to comply with the UK GDPR and other data protection laws.

• Monitor BDAT compliance with the UKGDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and ensuring BDAT and Trust employees receive appropriate training and data protection awareness communications.

The DPO will update the BDAT Trust Board on UKGDPR compliance, UKGDPR compliance will be overseen by the Audit and Risk Committee.

4.2 Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Processing is the collection, recording, organisation structuring, storage, adoption or alteration, retrieval, consultation or use, disclosure, destruction or erasure of personal data.

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

- **Legal Obligation** – The performance of a task for statutory/legal reasons
- **Public Interest** - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- **Contractual Obligation** - For the performance of a contract with the data subject or to take steps to enter into a contract e.g. Staff Contracts
- **Vital Interest** - Protecting the vital interests of a data subject or another person e.g. emergency medical situation
- **Legitimate Interest** - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks).
- **Consent** - Where processing cannot be categorised under the above conditions, the consent of the data subject must be held or obtained e.g. sharing photographs and news stories.

Special Categories of Data "Sensitive data" will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Where special category personal data is processed, BDAT will identify both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9.

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 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 set within law or a contract with a health professional.

• Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

• Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

4.3 Consent

Consent must be:	**Consent, cannot be obtained from the following:**
1.0 Freely given (a positive indication)	7.0 Silence
2.0 Specific	8.0 Pre-ticked boxes
3.0 Informed	9.0 Inactivity
4.0 An unambiguous indication of an individual's wishes	
5.0 A form of firm confirmation or positive opt-in, such as ticking boxes on a webpage	
6.0 Easily able to be withdrawn	

Where consent is given, a record will be kept documenting how and when consent was given on student records and staff files or other storage mechanism. This information must be readily available for staff to check that consent has been obtained e.g. use of student photographs.

BDAT and its academies schools must ensure that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

NOTE: Where processing is deemed to require "Consent", BDAT is aware that this "Consent" can be withdrawn by the individual at any time. It is therefore extremely important that academies consider any processing activities whereby data is shared or processed and becomes outside the control of BDAT, in these instances, specific "informed" consent will need to be obtained.

Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parent/carer (person with legal responsibility)/legal guardian) 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.

4.4 The right to be informed / Sharing Personal Data (Privacy Notices)

The UK GDPR requires BDAT to inform individuals if they collect, process, or share personal information about them. BDAT is also required to share personal information about its staff or students with other organisations, mainly with the local authority, other schools, and educational bodies, and potentially children's services and various contracted school services and systems.

We will issue Privacy Notices as outlined below. These are detailed in section 5 of this policy.

BDAT has adopted the DfE Model Privacy Notices for schools as the basis for the Privacy Notices and wherever possible will ensure that the privacy notice is written in a clear, plain manner.

4.5 The right of access

Individuals have the right to obtain confirmation that their data is being processed and the right to submit a data subject access request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of their records for other purposes.

When schools receive a request, the Academy Business Leader/DPC should follow the Trust Data Subject Access Request Procedures in the table within this section.

For individuals wishing to make a data subject access request. Although individuals are entitled to submit a DSAR to any member of staff, they should be made (if possible) to the Academy Business Leader of the academy, who in most cases, will be the Data Protection Coordinator. Requests can be made verbally and in writing.

Responses to SARs shall normally be made within one calendar month of receipt, however the trust holds the right to extend the period of compliance by up to a further two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed. Any extension will be dependent upon the terms of the UKGDPR, the Data Protection Act (2018) and associated ICO guidance.

In most cases when an individual makes a SAR you will need to ask for identification (ID) from them.

In a school setting, pupils and their parents or carers are generally well-known to school staff. If you know the requester and are sure of their identity and authority, you do not have to request ID. Make a record of why you made this decision.

If the requester is asking for their own information, and you do not know them, then they will need to provide their identification.

Adults should provide a photo ID plus another form of ID, this could be:

- their driving license or passport for the photo ID
- a utility bill or council tax bill that confirms their name and address

If the requester is asking for another individual's information, then they will need to provide the individual's ID.

They will also need to provide evidence that they have the authority to act on the individual's behalf. This includes requesters such as parents and solicitors.

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.

BDAT Data Subject Access Request Procedures:

Step	Action
1	**Data Subject Access Request from individual "Data Subject"**
2	**REQUEST RECEIVED?** ABL/DPC to forward to BDAT DPO for logging and review
3	**CHECK IDENTITY / Validity?** Is the individual known to the school? If not ABL/DPC to request form of ID and ID if for a child / proof of right to act on behalf of the individual.
4	ABL/DPC to send BDAT SAR acknowledgement letter
6	**IS THE REQUEST VALID/APPROVED? YES** - collate the information and send within 30 days from confirmation of ID. Send to DPO for final check/confirm an extension of up to two months before expiry. Use the BDAT response letter when sending the information . **NO** - Advise the Individual without delay of the decision or request further details to enable the request to be dealt with.
7	**PROVIDE THE INFORMATION** Supply information as per the agreed "secure" method. **NOTE**: Ensure only supply the actual data requested and that personal data or images of others are redacted/removed electronically

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

4.6 The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified and can do this through a request to the Academy Business Manager/Data Protection Coordinator. Upon receiving a request for rectification, the Trust or Trust school should take the following action immediately:

• Check the validity of the request e.g. confirm identity of the person requesting the change

• If the request is valid, amend the information where possible and record the actions taken

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

• Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to

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

• Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy

4.7 The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. If an individual wishes to exercise this right they should contact the Academy Business Leader/ Data Protection Coordinator.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

- **Where personal data has been disclosed to third parties**, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so
- **Where personal data has been made public within an online environment**, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question

4.8 The right to restrict processing

Individuals have the right to block or suppress the Trust or Trust school's processing of personal data. If an individual wishes to exercise this right they should contact the Academy Business Leader/Data Protection Coordinator

Such a restriction may affect the Trust or Trust school carrying out their legal and contractual obligations. It may also be believed that the data is being processed under the public interest, vital Interest or legitimate interest conditions of processing. In these circumstances guidance from the DPO and/or the Information Commissioner's Officer to determine that the request is valid should be sought.

In the event that request is valid and the processing is restricted, the school 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.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
- If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so

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

4.9 The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. If an individual wishes to exercise this right they should contact the Academy Business Leader/Data Protection Coordinator. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

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

- 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

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

The school will provide the information free of charge, and;

- Where feasible, data will be transmitted directly to another organisation at the request of the individual
- The school is not required to adopt or maintain processing systems, which are technically compatible with other organisations
- In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual
- The school will respond to any requests for portability within one month
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of

the extension and the reasoning behind it within one month of the receipt of the request
- Where no action is being taken in response to a request, the school 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

4.10 The right to object

The school 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. If an individual wishes to exercise this right they should contact the Academy Business Leader/Data Protection Coordinator.

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

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

- An individual's grounds for objecting must relate to his or her particular situation
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

Where personal data is processed for direct marketing purposes:

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

Where personal data is processed for research purposes:

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

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

4.11 Automated decision making and profiling

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
- The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it

When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent/carer (person with legal responsibility)/legal guardian 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

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

- The school has the explicit consent of the individual
- The processing is necessary for reasons of substantial public interest on the basis of UK law.

4.12 Privacy by design and privacy impact assessments

The key aims of Privacy by Design are:-

- Proactive not reactive measures
- Privacy as a default setting
- Privacy embedded
- Privacy throughout project life cycle

The school will act in accordance with the UKGDPR by adopting a privacy by design approach and implementing technical and organisational measures, which demonstrate how the Trust and Trust schools have considered and integrated data protection into their processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation, which might otherwise occur.

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.

Where a DPIA indicates high-risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the UKGDPR.

Trust employees should follow the Trust Data Protection Impact Assessment (DPIA) Procedure

4.13 Data breaches

Trust employees should follow the Trust Data Breach Management procedures.

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

- All personal data breaches must be reported immediately to the Academy Business Leader/Data Protection Coordinator, who should them immediately report to the Trust DPO (Deputy CFO)

- If a personal data breach occurs and that breach is likely to result in a high risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. This decision will be made in line with ICO guidance.

- In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Trust Breach Management Procedures:

Step	Action
1	**DATA BREACHES SHOULD BE REPORTED IMMEDIATELY TO**: The Academy Business Leader/Data Protection Coordinator. Breach should then be reported to DPO.
2	Academy Business Leader/Data Protection Coordinator to complete BDAT Data breach form which includes an early investigation
3	BDAT DPO to log and determine risk
4	If determined to be ICO notifiable, the ICO will be notified within 72 hours by the BDAT DPO
5	In all high risk breaches, an investigation will be carried out by the BDAT DPO
6	Any recommendations for improvement will be shared and control measures implemented
7	In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Academy Business Leader will ensure that all affected data subjects are informed of the breach directly and without undue delay. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

4.14 Third party processors/ Other authorised persons

The Trust requires all third party processors who have access to or process personal data on behalf of the Trust, to provide written confirmation that they will comply with the requirements of the UKGDPR and maintain adequate physical and IT security controls to protect our data.

We will request contractors, suppliers, and system providers who may process our personal data to provide written assurance/contract terms to confirm that:-

- Any personal data you receive from us in the course of your performance of the relevant contract or service level agreement will only be processed in accordance with our documented instructions.
- No personal data will be transferred to any country outside the EEA or any international organisation without obtaining our prior written consent
- No third party will be engaged to carry out any processing activities in respect of the personal data without our prior written consent, and if consent is given, the third party will be subject to a written contract containing the same data protection obligations as set out between you and us in the contract or service level agreement, and the provisions of this letter.
- Appropriate organisational and technical security measures are in place to protect any personal data, which may be processed or handled under the contract or service level agreement, and to assist us in complying with our obligations to deal with requests from data subjects to exercise their rights under the UKGDPR.

• Appropriate systems to investigate and report data breaches are in place and that all breaches will be notified to the DPO immediately and the ICO within 72 hours (where relevant).
• You will assist us in complying with our obligations in relation to security of processing, dealing with data breaches and carrying out privacy impact assessments.
• When the services under the contract or service level agreement end, you will (at our option) delete or return all personal data and copies of the same.
• You will make information demonstrating compliance with the above obligations available to us on request and will allow for and contribute to any audits or inspections that we may conduct.

We will seek written confirmation from other authorised persons e.g. job applicants, students, volunteers, contractors, freelancers, board members, LSC members that they will comply with Trust and School policies and procedures and that we expect appropriate physical and IT data security controls to be exercised if given access to personal data and systems.

4.15 Data security

BDAT are working towards the Cyber Essentials Accreditation to demonstrate our IT Security Management Systems are effective. We also comply with the RPA requirements regarding offline back-ups, National Cyber Security Centre training, registration with the Police scheme 'Cyber Alarm' and having a Cyber Response Plan.

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

BDAT, its employees and others with authorised access to personal data will ensure that appropriate IT and physical data security controls are used to protect unauthorised access to confidential records e.g.

1. Keep passwords secure, regularly change them and don't share with others.
2. Lock PC/Laptop screen or log off when away from your desk.
3. Position computer screens so they are not visible to "unauthorised persons" when in use.
4. Exercise caution when using Laptops in public areas and only connect to secure Wi-Fi connections.
5. Be aware of who can overhear sensitive conversations, take necessary precautions.
6. Operate a "Clear Desk Policy" and securely store papers/files that contain personal data when not in use.
7. Be careful when opening emails and attachments if you don't recognise the sender or the heading looks suspicious) or visiting new websites e.g. virus aware.
8. Dispose of personal data securely e.g. shred/confidential waste bin.
9. Encrypt or password protect personal information on attachments/devices/memory sticks. 10.Update personal data as soon as you are made aware of any changes e.g. notify the Admin/HR Team.
10. Ensure old devices/laptops/hard drives are given to IT/Academy Business Leaders to dispose of securely.

11. Follow Trust Data Sharing Guidance and check there is a legal basis or that we have a Privacy Notice or Data Subject Access Request before sharing personal information about staff, students and others.
12. Report breaches or potential breaches and fraudulent attempts to access data.

4.16 CCTV and photography

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

CCTV

Trust staff will follow the Trust CCTV Protocol for information in relation to the use and purpose of CCTV monitoring in schools.

Photographs and non-CCTV recording images

The Trust will request consent for taking photographs and recording/videoing of students, staff and others and will only use them for the purposes covered on the appropriate Trust Privacy Notices. If the Trust or Schools require to use images for any other purpose, permission will obtained from the individual or for students, the parent/carer (person with legal responsibility/legal guardian) if under the age of consent.

Images/Videos captured by individuals for recreational/personal purposes

For clarification, images captured by individuals for recreational/personal purposes, and videos made by a parent/carer for family use, are exempt from the UKGDPR, however, the Trust and Schools do require that permission be obtained from the Trust/school beforehand

4.17 Data retention

Under the UKGDPR, Data must not be kept for longer than is necessary. It is therefore extremely important that the Trust and schools have effective policies and procedures in place to ensure the timely secure disposal or deletion of data e.g. paper records disposed of via confidential waste bins and appropriate IT controls for electronic data.

Some records relating to former students or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts

Trust employees will follow the guidance set out in the Trust Data Retention Schedule

Bradford Diocesan Academies Trust

5.0 Pupil Privacy Notice

5.1 Pupil Privacy Notice

When collecting and using personal data relating to pupils and their families, BDAT complies with the requirements of Data Protection Legislation (being the UK General Data Protection Regulation, Data Protection Act 2018 and The Privacy and Electronic Communications (EC Directive) Regulations 2003) and all other applicable laws and regulations relating to processing of personal data and privacy, as amended and replaced from time to time.

For the purpose of Data Protection requirements, the data controller is BDAT. This means our schools determine the purposes and means for which any personal data is to be processed.

We are registered as a Data Controller with the ICO: Ref ZA025705

Each school has a GDPR Coordinator who acts as a representative for the school with regard to its data controller responsibilities.

Matthew Hill is the Data Protection Officer (DPO). This role is to oversee and monitor the Trust's data protection procedures, and to ensure they are compliant with the Data Protection Legislation. The Data Protection Officer can be contacted on 01274 909 120

The categories of personal data that we collect, hold and share include:

- personal identifiers and contacts (such as name, unique pupil number, contact details, date of birth, identification documents, next of kin, and emergency contacts)
- characteristics (such as ethnicity, language and eligibility for free school meals)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors' information, child health, dental health, allergies, medications, dietary requirements, and accident records)
- attendance (such as sessions attended, number of absences, absence reasons and at previous schools attended)
- results of internal assessments and externally set tests
- pupil and curricular records
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- details of any support received, including care packages, plans and support providers
- use of internet and ICT resources in school
- photographs and moving images
- images on our surveillance systems (such as CCTV images captured in and around our premises).

Why we collect and use this information:

We collect and use personal data as set out under the UKGDPR and UK law. We use this data:

- to support teaching and learning
- to monitor and report on pupil attainment progress

- to provide appropriate pastoral care
- to assess the quality of our services
- to protect pupil welfare
- to keep children safe (food allergies, or emergency contact details)
- to safeguard pupils
- to enable pupils to take part in national or other assessments and to publish the results of public examinations or other achievements of pupils
- to share news about our work and promote our services
- to arrange educational visits and extracurricular activities for pupils
- enable us to carry out specific functions for which we are responsible
- to comply with the law regarding data sharing
- to meet the statutory duties placed upon us for the Department of Education (DfE) data collections.

Legal basis for using your personal information

We must make sure that information we collect and use, is in line with the UK GDPR and Data Protection Act. This means that we must have a lawful reason to collect the data and that if we share it with another organisation or individual we must have a legal basis to do so.

Under the UK GDPR, processing of the data held is lawful if at least one lawful basis applies. The bases which we rely on for processing personal information, which is collected and used for the reasons listed above, are as follows:

- Consent (Article 6(1)(a)) – we have permission from you to process the personal data. You do have the right to withdraw your consent at any time.
- Contract (Article 6(1)(b)) – we collect and process personal data necessary for the performance of a contract.
- Legal Obligation (Article 6(1)(c)) – we collect and process personal data so we can comply with the law.
- Vital Interests (Article 6(1)(d)) - collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk.
- Public Task (Article 6(1)(e)) - we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours.
- Legitimate Interest (Article 6(1)(f)) - for the purposes of our legitimate interest.

We may process personal information based on legitimate interests, provided that such interests are not overridden by your rights and freedoms. In the context of the school, our legitimate interests include:

- Ensuring the effective operation and administration of the school, including the coordination of teaching, learning, and extracurricular activities.
- Protecting the safety and welfare of pupils, staff, and visitors, including monitoring school premises.
- Maintaining the security and efficient functioning of school systems, networks, and data.
- Conducting internal audits, investigations, and due diligence as needed.

Where we are required to collect special category data, we will use the following lawful bases of the UK GDPR which permits us to process special category data:

- Explicit Consent (Article 9(2)(a)) – we may request explicit consent from individuals (or parents/guardians in the case of minors) to process special category data for specific purposes, such as, using biometric information to identify individuals to school IT systems
- Employment, Social Security, and Social Protection (Article 9(2)(b)) – we may process special category data necessary for fulfilling obligations in the fields of employment law, social security, or social protection, such as medical conditions, allergies, or disabilities, to comply with laws that require them to ensure a safe environment.
- Vital Interests (Article 9(2)(c)) – in situations where processing is essential to protect someone's life, such as during a medical emergency, schools may process special category data without prior consent.
- Made public by the data subject (Article 9 (2)(e)) - to process special category data if that data has been manifestly made public by the data subject.
- Legal claims (Article 9(2)(f)) – where the processing is for the purposes of establishing, exercising, or defending legal claims or by courts when they are acting in their judicial capacity.
- Substantial Public Interest (Article 9(2)(g)) – we often process special category data in the public interest, for instance, to comply with equality legislation, ensure diversity and inclusion, or meet safeguarding obligations.
- Provision of Health or Social Care (Article 9(2)(h)) – we may collect health-related data to provide appropriate health care services or health management for pupils, such as managing disability accommodations or providing necessary medical care
- Archiving, Research, or Statistical Purposes (Article 9(2)(j)) – we may process special category data for academic research, statistical purposes, or archiving in the public interest, provided that appropriate safeguards are in place.

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

Collecting personal information

Collecting pupil data is essential for our schools' operational use. Whilst the majority of pupil information you provide to us is compulsory, we do request some on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

Most of the personal information we process is provided to us by you for one of the following reasons:

- You have enrolled a pupil
- You wish to attend, or have attended, an event organised by us
- You have made an enquiry to us
- You have made a complaint to us
- You have made an information request to us.

We also receive personal information indirectly, for example:

- We have contacted another organisation about a pupil, and it gives us personal information in its response.

- Personal information is contained in reports from other agencies such as Local Authority or the NHS
- A complainant refers to you in their complaint correspondence
- Other parents include information about you in their reporting to us
- From other public authorities, regulators, or law enforcement bodies.

Storing personal information

In accordance with the UK GDPR, the school does not store personal data indefinitely. We will only use and store personal information for as long as it is required for the purposes it was collected for.

All personal information is kept secure either on encrypted, password protected devices and systems, or paper copies kept on the school site. Once the deadline for retaining information has passed, data stored electronically is deleted and paper copies destroyed

Who and why we share information with

We routinely share information with:

- Educational institutions that the pupils attend after leaving us
- The Local Authority – for admissions, exclusions and safeguarding
- The Department for Education (DfE) – see section below
- Trust staff
- The pupil's family and representatives
- Parents or carers of Trust school pupils
- Educators and examining bodies
- Ofsted
- 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
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Media publications
- Police forces, courts, tribunal
- Youth Support Services (Pupils aged 13+) – see section below.

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

When we use suppliers and service providers to process information, we ask them to demonstrate compliance with our security requirements, adhere to any instructions we give them and comply with relevant data protection legislation. We have contractual agreements with these organisations which clearly define their obligations about what information they hold

Youth Support Services
Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil 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 through youth support services and careers advisers.

The information shared is limited to the child's name, address, and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child/pupil once they reach the age 16.

Pupils aged 16+

We will also share certain information about pupils 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 via post-16 education and training providers, Youth Support Services and careers advisers.

For more information about services for young people, please visit www.bradford.gov.uk.

Department for Education (DfE)

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls, which meet the current government security policy framework.

How Government uses your data

The pupil data that we lawfully share with the Department for Education (DfE) through data collections:

• underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
• informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
• supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school).

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education (DfE) and contains information about pupils in schools in England. This information is securely collected from a range of sources including schools, local authorities and awarding bodies

The data in the NPD is provided as part of the operation of the education system and is used for research and statistical purposes to improve, and promote, the education and well-being of children in England.

The evidence and data provide DfE, education providers, Parliament and the wider public with a clear picture of how the education and children's services sectors are working in order to better target, and evaluate, policy interventions to help ensure all children are kept safe from harm and receive the best possible education.

Sharing by the Department for Education (DfE)

DfE will only share pupils' personal data where it is lawful, secure and ethical to do so. Where these conditions are met, the law allows the Department for Education (DfE) to share pupils' personal data with certain third parties, including:

- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime.

Organisations fighting or identifying crime may use their legal powers to contact the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

How to find out what personal information the Department for Education (DfE) holds about you

Under the terms of the UK GDPR, you are entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

Requesting your personal information from the Department for Education - GOV.UK

Requesting access to your personal data

The UK GDPR gives parents and pupils certain rights about how their information is collected and used. To make a request for your personal information, or be given access to your child's educational record, contact the relevant school

You also have the following rights:

- Right to be informed – to be informed about how and why we process your personal information.
- Right of access - to ask for copies of your personal data that we hold about you, this is known as a subject access request (SAR), data subject access request or right of access request.
- Right of rectification - to ask us to change any information you think is not accurate or complete.
- Right to erasure - to ask us to delete your personal information.
- Right to restriction of processing – to ask us to stop using your information.
- Right to object to processing of your information, in certain circumstances.
- Right of data portability - allows individuals to obtain and reuse their personal data for their own purposes across different services.
- Rights related to automated decision-making including profiling.
- Right to withdraw consent at any time (where relevant).
- Right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- Right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- Right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- Right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent.

Complaints and Concerns

If you would like to discuss anything on this Privacy Notice or are unhappy with the way your request for information has been dealt with or you think your data has been misused or not held securely, please contact: BDAT DPO, 01274 909120

If you are unhappy with the outcome of your query or complaint, you can escalate your complaint please contact the Information Commissioner's Office (ICO). ICO helpline, Telephone: 0303 123 1113 https://ico.org.uk/concerns/

5.2 Workforce Privacy Notice

When collecting and using personal data relating to employees and other individuals engaged in work, BDAT complies with the requirements of Data Protection Legislation (being the UK General Data Protection Regulation, Data Protection Act 2018 and The Privacy and Electronic Communications (EC Directive) Regulations 2003) and all other applicable laws and regulations relating to processing of personal data and privacy, as amended and replaced from time to time.

For the purpose of Data Protection requirements, the data controller is BDAT. This means our schools determine the purposes and means for which any personal data is to be processed.

We are registered as a Data Controller with the ICO: Ref ZA025705

Each school has a UK GDPR lead who acts as a representative for the school with regard to its data controller responsibilities.

Matthew Hill is the Data Protection Officer (DPO). This role is to oversee and monitor the Trust's data protection procedures, and to ensure they are compliant with the Data Protection Legislation. The Data Protection Officer can be contacted on 01274 909120

What personal information do we process?

The categories of workforce information that we collect, process, hold and share include:

- Personal information (such as name, address, employee or teacher number, national insurance number)
- Marital Status
- Special categories of data including characteristics information such as gender, age, ethnic group
- Employment terms and conditions and contract information (such as start dates, hours worked, post, roles, benefits, absence, holidays, and salary information)
- Emergency contact details
- Details of any known disability or medical condition
- Education and qualifications
- Recruitment information, including copies of right to work documentation, references and other information collected as part of the application process
- Outcome of disciplinary or grievance procedures
- Performance and appraisal data
- Work experience
- Accident information
- Training information
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Payroll information
- Photographs and video
- CCTV images captured in school premises

- Use of internet and ICT resources on school services and devices
- Biometric data in some settings (for cashless catering)

Why we collect and use this information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed (including, but not limited to, internal management planning and forecasting, and statistical analysis such as diversity or gender pay gap analysis as required by law)
- Inform the development of recruitment and retention policies
- Enable individuals to be paid
- Enable us to carry out specific functions for which we are responsible
- Ensure the safeguarding of students and staff and comply with relevant legislation
- Ensure we comply with relevant legislation e.g. Health and Safety at Work Act
- To operate school systems e.g. cashless catering and security systems e.g. door entry systems and swipe-cards
- Supporting the work of the School Teacher Review Body and the School Support Staff Negotiating Body
- Enable us to deal with any disciplinary action and grievances
- Share news about our work and promote our services
- Assess the quality of our service
- Fulfil our contractual obligations
- the purposes of crime prevention and security.

The lawful basis on which we process this information

We must make sure that information we collect and use, is in line with the UK GDPR and Data Protection Act. This means that we must have a lawful reason to collect the data and that if we share it with another organisation or individual, we must have a legal basis to do so.

Under the UK GDPR, processing of the data held is lawful if at least one lawful basis applies. The bases which we rely on for processing personal information, which is collected and used for the reasons listed above, are as follows:

- Consent (Article 6(1)(a)) – we have permission from you to process the personal data. You do have the right to withdraw your consent at any time.
- Contract (Article 6(1)(b)) – we collect and process personal data necessary for the performance of a contract.
- Legal Obligation (Article 6(1)(c)) – we collect and process personal data so we can comply with the law.
- Vital Interests (Article 6(1)(d)) - collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk.
- Public Task (Article 6(1)(e)) - we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours.

We process personal data in order to meet the requirements set out in UK employment, academy and safeguarding law, including those in relation to the following:

- Academy Funding Agreement and Articles of Association
- Academy's legal and statutory framework
- Safeguarding Vulnerable Groups Act 2006
- The guidance "Keeping Children Safe in Education"
- The Childcare (Disqualification) Regulations 2009

Where we are required to collect special category data, we will use the following lawful bases of the UK GDPR which permits us to process special category data:

- Explicit Consent (Article 9(2)(a)) – we may request explicit consent from individuals to process special category data for specific purposes, such as, using biometric information to identify individuals to school IT systems
- Employment, Social Security, and Social Protection (Article 9(2)(b)) – we may process special category data necessary for fulfilling obligations in the fields of employment law, social security, or social protection, such as medical conditions, allergies, or disabilities, to comply with laws that require them to ensure a safe environment.
- Vital Interests (Article 9(2)(c)) – in situations where processing is essential to protect someone's life, such as during a medical emergency, schools may process special category data without prior consent.
- Made public by the data subject (Article 9 (2)(e)) - to process special category data if that data has been manifestly made public by the data subject.
- Legal claims (Article 9(2)(f)) – where the processing is for the purposes of establishing, exercising, or defending legal claims or by courts when they are acting in their judicial capacity.
- Substantial Public Interest (Article 9(2)(g)) – we often process special category data in the public interest, for instance, to comply with equality legislation, ensure diversity and inclusion

In addition, we rely on processing conditions of Schedule 1 part 1 of the Data Protection Act 2018. This relates to the processing of special category data for employment purposes.

How do we get your information?

BDAT collects information about you from the following sources:

- Directly from you
- From an employment agency
- From referees, either external or internal
- From security clearance providers
- From Occupational Health and other health service providers
- From Pension administrators and other government departments, for example tax details from HMRC
- From your Trade Union
- Images from our own Surveillance Systems (CCTV)

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

In accordance with the UK GDPR, data is only stored for as long as is necessary for the purpose it was originally collected. We hold data securely for the set amount of time shown in our Data Retention Schedule.

We will not transfer your data outside the European Economic Area ("EEA").

All personal information is kept securely either on encrypted, password protected devices and systems, or paper copies kept on the school site. Once the deadline for retaining information has passed, data stored electronically is deleted and paper copies destroyed.

Who we share this information with

We routinely share this information with:

- Our Local Authority
- The Department for Education (DfE)
- Trust staff
- The pupil's family and representatives
- Parents or carers of Trust school students
- Educators and examining bodies
- Regulatory Bodies, such as Ofsted
- 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
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Media publications
- Police forces, courts, tribunals.

When we use suppliers and service providers to process information, we ask them to demonstrate compliance with our security requirements, adhere to any instructions we give them and comply with relevant data protection legislation. We have contractual agreements with these organisations which clearly define their obligations about what information they hold

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 educational attainment.

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

How Government uses your data

The workforce data that we lawfully share with the Department for Education (DfE) through data collections:

- informs the Department for Education (DfE) policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

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-andcensuses-for-schools

Sharing by the Department for Education (DfE)

The Department for Education (DfE) 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 for Education (DfE) will only share your personal data where it is lawful, secure and ethical to do so and 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 the Department for Education (DfE) releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of public benefit, proportionality, legal underpinning and strict information security standards.

How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of UK GDPR, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to

- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department of Education (DfE), you should make a 'subject access request'.

To contact the Department for Education (DfE): https://www.gov.uk/contact-dfe

Rights in relation to your personal data

The UK GDPR gives all individuals certain rights about how their information is collected and used. To make a request for your personal information, contact the Academy Business Leader/Data Protection Coordinator at the relevant school.

You also have the following rights:

- Right to be informed – to be informed about how and why we process your personal information
- Right of access - to ask for copies of your personal data that we hold about you, this is known as a subject access request (SAR), data subject access request or right of access request.
- Right of rectification - to ask us to change any information you think is not accurate or complete.
- Right to erasure - to ask us to delete your personal information.
- Right to restriction of processing – to ask us to stop using your information.
- Right to object to processing of your information, in certain circumstances.
- Right of data portability - allows individuals to obtain and reuse their personal data for their own purposes across different services.
- Rights related to automated decision-making including profiling.
- Right to withdraw consent at any time (where relevant).
- Right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- Right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- Right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- Right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent.

Complaints and Concerns

If you would like to discuss anything on this Privacy Notice or are, unhappy with the way your request for information has been dealt with or think your data has been misused or not held securely, please contact:

Matthew Hill, Data Protection Officer

Tel: 01274 909120

If you are unhappy with the outcome of your query or complaint, you can escalate your complaint please contact the Information Commissioner's Office (ICO). ICO helpline, Telephone: 0303 123 1113 https://ico.org.uk/concerns

Bradford Diocesan Academies Trust

Appendix 1: Data Protection Impact Assessment Template

Data Protection Impact Assessment Form (DPIA)

The purpose of completing a Data Protection Impact Assessment (DPIA) is to consider the risks and the potential harm that may arise both for the individuals concerned and the organisations involved. When considering your project please ensure that you are processing and sharing the minimal amount of personal data possible and ensure that the processing is fair, lawful and transparent. You must also ensure you have reasonable security measures in place to protect the personal data you are processing.

Please provide the information requested below (see sections in grey). The Data Protection Officer will need to have a basic understanding of your overall project and more detailed information about how you will be processing personal data as part of that. Please try and keep your answers brief whilst addressing the points requested in the questions. It is your responsibility to complete the form with the required information. Once you have submitted the completed form to the Data Protection Officer (matthew.hill2@bdat-academies.org), please wait for confirmation that the project can progress.

Project Title:
Name of responsible person:
Date form completed:

1) Project details	
Provide a brief description in the box below of the project including an explanation of what the project aims to achieve (~half page, maximum one page). Your description should highlight those features that may have a potential impact on privacy. Your description should cover the following points (when you have completed your description please check the boxes to confirm these items have been covered in your text, or if it is not applicable record this):	
☐ A description of who the data subjects will be;	or ☐ Not Applicable
☐ An estimation of the number of data subjects whose information will be processed;	or ☐ Not Applicable
☐ Whether any vulnerable adults or children are involved;	or ☐ Not Applicable
Enter text here	

2) Justification, purpose and necessity
Please briefly explain why the processing is necessary, whether any alternative solutions have been considered, what the benefits of the processing are and what you hope to achieve that could not be achieved in other ways that did not involve the processing of personal data.

3) Details of personal data
Please indicate what personal data will be collected/stored/processed.
Administration data ☐ Name ☐ Date of Birth/Age ☐ Gender ☐ Contact details ☐ Unique identifier e.g. student number

3) Details of personal data
☐ Other data (please specify): *Special Categories of data (If you tick any of the boxes in this section please ensure you answer question 5 below)* ☐ Racial or ethnic origin ☐ Political opinion ☐ Religious or philosophical beliefs ☐ Trade Union membership ☐ Physical or mental health condition ☐ Sexual life and sexual orientation ☐ Genetic data ☐ Biometric data used to identify an individual *Other sensitive information* ☐ Financial information/bank account details ☐ Criminal convictions and offences *(If you tick this box please ensure you answer question 5 below)* ☐ Other (please specify):

4) Lawful Basis for processing (Article 6)
Under Article 6 of the UK GDPR there needs to be a lawful basis for processing personal data. Further details about this are available in section 4.2 oF the BDAT GDPR policy. Having read the guidance please indicate the lawful basis that will apply to your project. If you need additional advice on this please speak to the BDAT Data Protection Officer
☐ The individual who the personal data is about has given/will give unambiguous consent to the processing ☐ The processing is necessary for the performance of a contract with the individual

4) Lawful Basis for processing (Article 6)
☐ The processing is necessary for a legal obligation
☐ The processing is necessary for the vital interests of someone (i.e. life or death situation)
☐ The processing is carried out in the public interests or in the exercise of official authority
☐ The processing is in the legitimate interests of the Academy or another party and does not prejudice the rights and freedoms of the individual

5) Lawful Basis for processing special category or criminal conviction data (Article 9 or 10)
If you are processing 'Special Category' personal data or criminal conviction data (see question 3 above) you will require a separate lawful basis for processing this type of data under Article 9 of UK GDPR and/or you will need to meet one of the conditions in Schedule 1 of the Data Protection Act 2018. If this applies to your project please contact the BDAT DPO.

6) Describe the Personal Data and Information flows	
The collection, use and deletion of personal data should be described here. Where you have different groups of data subjects (e.g. staff and students) and their data will be handled in different ways please cover in your explanation the flows for each set of personal data. Your description should cover the following points (when you have completed your description please check the boxes to confirm these items have been covered in your text, or if it is not applicable record this):	
☐ Explain where your personal data is coming from (new data or existing data);	or ☐ Not Applicable
☐ How the data will be collected or obtained;	or ☐ Not Applicable
☐ How the data will be stored securely;	or ☐ Not Applicable
☐ What systems will be used;	or ☐ Not Applicable
☐ How long the data will be retained for;	or ☐ Not Applicable
☐ How will personal data be disposed of when no longer required;	or ☐ Not Applicable
☐ Who will have access to the data;	or ☐ Not Applicable
☐ What security measures will be in place;	or ☐ Not Applicable
☐ Explain what third parties will have access to the data and confirm suitable contracts are in place;	or ☐ Not Applicable

6) Describe the Personal Data and Information flows	
☐ Explain the context of any questions on the Screening Form which were marked as 'Yes';	or ☐ Not Applicable
☐ Any other relevant information;	or ☐ Not Applicable
Enter text here	

7) Transparency, Privacy Notices and Consent
Please explain what arrangements will be put in place to inform individuals what you are planning to do with their personal data or get their consent. You need to ensure that your proposed activity is already covered within the BDAT privacy notice, section 5 of the BDAT GDPR policy. If the lawful basis for processing personal data is consent (see section 4) please explain how you will be obtaining and recording consent.

8) Identification of privacy and related risks and solutions
In this section you should identify the key privacy risks and associated compliance and corporate risks. Examples of risks are outlined below but they may or may not be relevant to your project. Please consider your project carefully to identify what risks should or should not be included and amend the grey text accordingly. In addition, there may be specific risks not mentioned below that require consideration. Risks could result in unnecessary intrusion on privacy, risks to physical safety, financial loss or distress caused. Privacy legislation for consideration may include: The Data Protection Act 2018 and UK General Data Protection Regulation (GDPR) – Regulate the processing of personal data – i.e. information about living identifiable individuals Privacy and Electronic Communications Regulations 2003 (PECR) - Regulates electronic direct marketing e.g. email and text messages Human Rights Act 1998 – Individual's right to respect for their private and family life, their home and correspondence.

Bradford Diocesan Academies Trust

8) Identification of privacy and related risks and solutions					
The Common Law Duty of Confidence You should also identify solutions and thereafter balance the project's outcomes with the impact on individuals. Whilst some risks might be eliminated altogether, other risks might be reduced and it may be appropriate to recognise and accept the risks. Each residual risk should thereafter be evaluated against the likelihood of harm to individuals and the severity of possible harm.					
Privacy issue/ Risk	**Risk to individuals**	**Compliance/ organisation/ corporate risk (see table at the end of the form for examples of relevant privacy legislation)**	**Solutions and actions to be taken**	**Evaluation of residual risks after implementing solutions**	
				Likelihood of harm to individuals: **1 - Rare** **2 - Unlikely** **3 - Moderate** **4 - Likely** **5 - Almost Certain**	**Severity of harm:** **A - Insignificant** **B - Minor** **C - Moderate** **D - Major** **E - Extreme**
Compliance with the data subject's right to be informed	The individuals will not be aware of how their personal data will be processed, who it will be shared with etc	Potential to breach the first data protection principle of 'lawfulness, fairness and transparency'/reputational risk/financial risk	Explain how you will be informing the data subjects what will be happening with their personal data i.e. have you got privacy notice relating to the project. What are your arrangements for getting consent where required.		
Personal data is used for a purpose which is incompatible with the purpose it was originally collected	The individuals will not be aware of how their personal data will be processed	Potential to breach the second data protection principle 'purpose limitation'. This will result in potential reputational	Explain what measures will be taken to prevent data being used for a purpose not outlined in the privacy notice. For data obtained from a different project or organisation will		

8) Identification of privacy and related risks and solutions					
for. e.g. existing data is being used for a new purpose or there is a risk that data collected is used in a way that data subjects would not expect		risk/financial risk to the Academy.	the individuals be re-contacted to explain how their information will be re-used?		
There is a risk that more personal information is gathered or held as part of the project than is actually needed.	More information is collected from individuals than is required. This could lead to stress of the individuals concerned.	Potential to breach the third data protection principle 'data minimisation'. This will result in potential reputational risk/financial risk to the Academy	Explain the measures that will be taken to ensure only the minimal data is collected and what data minimisation techniques will be implemented such as anonymisation.		
The personal data held is inaccurate	Risk of holding incorrect data potentially leading to inaccurate conclusions or decision to be taken.	Potential to breach the fourth data protection principle 'accuracy'. This will result in reputational risk/financial risk to the Academy	Explain what processes will be in place to ensure data is accurate and kept up to date? For instance allowing data subjects to access their own data on a system to keep information up-to-date?		
Personal data is held for longer than is necessary in breach of the storage limitation and data retention principle.	Personal information held by the Academy for longer than is needed causes distress to the	Potential to breach the fifth data protection principle 'storage limitation' This could result in reputational	Explain what the retention timescales will be and what methods will be used to delete or destroy data when it is no longer required? Confirm this information is in the privacy notice.		

8) Identification of privacy and related risks and solutions					
	individuals concerned.	risk/financial risk to the Academy			
Personal data is not held securely. Confidentiality, integrity and availability of personal data.	The information is not held securely and is breached. This could lead to people having access to the information who should not have access putting the security of individuals at risk.	Potential to breach the sixth data protection principle 'integrity and confidentiality'. This could result in a data breach and resultant reputational risk/financial risk to the Academy	Outline here all the controls in place to safeguard the personal data against a data breach. For example, relevant training for people accessing the data, access controls, password protection, encryption, pseudonymisation/ anonymisation, storage location, locking procedures, details of how the personal data will transmitted/shared.		
Third parties having access to the personal data	Measures are not in place to protect the security of personal data when it is passed to third parties.	Potential breach of Articles 24-43 (Controller and Processor responsibilities)	Are data processing contracts/data sharing/service agreements in place to assign responsibilities and liabilities?		
International Transfers. Personal data is transferred to a recipient outside of the UK/EU/EEA and located within a country that may not have adequate data protection laws.	The security of personal data could be put at risk as a result of the transfer leading to a risk for the individuals concerned.	Potential breach of Article 44 relating to transfers of personal data to third countries.	Explain what safeguards are in place to meet the requirements for transferring data internationally, e.g. having an International Data Transfer Agreement (IDTA) in place.		

8) Identification of privacy and related risks and solutions					
Complying with data subject rights including subject access requests	There is a risk that individuals will not be able to exercise their rights such as right to access, rectification, erasure, portability and right to object.	Potential breach of the data subject rights Articles 15-23	What measures are in place to ensure rights request could be handled, for instance extracting information relating to an individual from a system or deleting their information if it was no longer required.		
Consider your own project and add additional risks as appropriate					
Add further risks here					
Add further risks here					
Add further risks here					

9) Sign Off
The proposed solutions to the risks identified above must be approved by the DPO/Deputy DPO ☐ The proposed solutions have been reviewed and agreed by the DPO Name: Position:

In the event that any aspect of the project changes then the form should be updated and resubmitted

Please submit a copy of the completed form to the DPO matthew.hill2@bdat-academies.org
