BRADFORD ACADEMY TRUST

Responsibility | Respect | Resilience

Our **Vision** **RESPONSIBILITY** **RESPECT** **RESILIENCE**	**A shining light in our community** You are the light of the world. A city on a hill cannot be hidden. - Matthew 5:14b

Data Protection Policy

Approved by:	RMC	**Date:** December 2025
Last reviewed on:	December 2025	
Next review due by:	December 2026	
Related Documents		
Guidance	General data protection policy	
Author	**Data Protection Team**	

TABLE OF CONTENTS

1 INTRODUCTION AND SCOPE

Bradford Academy is required to process personal information about staff, pupils, parents, guardians, and other individuals we may interact with. We must do this in compliance with data protection and other relevant legislation.

This policy provides a framework for ensuring that we comply with the requirements of the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), and other relevant legislation, as well as associated guidance and codes of practice.

This policy, including its appendices, applies to our entire workforce. This includes employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for or on our behalf. Individuals found to knowingly or recklessly infringe this policy may face disciplinary action.

This is our main information governance policy and applies to all personal data, whether paper or electronic. It should be read alongside the other policies within our information governance policy framework.

2 ROLES AND RESPONSIBILITIES

Overall responsibility for ensuring that we meet the statutory requirements of any data protection legislation lies with the Board of Governors or Trustees. The following roles will have day-to-day responsibility for compliance and providing the necessary assurance to the Board.

2.1 DATA PROTECTION OFFICER (DPO)

The role of the DPO is to assist us in monitoring compliance with data protection legislation and advise on data protection issues. Bradford Academy have appointed Veritau as our DPO. Veritau's contact details are:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

The DPO service is an advisory role, and its duties include:

- Informing and advising us and our employees about our obligations to comply with the UK GDPR, the Data Protection Act 2018, and other data protection and information access laws;
- Monitoring compliance with data protection legislation and other information governance policies;

- Raising awareness of data protection issues; and
- Liaising with the Information Commissioner's Office (ICO).

2.2 SENIOR INFORMATION RISK OWNER (SIRO)

The SIRO is a senior staff member who is ultimately responsible for information risk. The SIRO will ensure that our information governance policies and procedures are effective and comply with legislation, promote best practice, and embed a culture of data protection compliance. In our organisation, this role lies with the Executive Principal

2.3 DATA PROTECTION TEAM (DPT)

The DPT take on the duties of what is also commonly referred as 'Single Point of Contact (SPOC)'. The DPT are a number of senior staff members who are ultimately responsible for information risk. The DPT will ensure that our information governance policies and procedures are effective and comply with legislation, promote best practice, and embed a culture of data protection compliance. In our organisation, this role lies with the IT Director, Data Manager and Finance Director.

The DPT will take operational responsibility for data protection compliance, including communicating with data subjects and the DPO service.

2.4 INFORMATION ASSET OWNER (IAO)

An IAO is an individual responsible for the security and maintenance of a particular information asset and for ensuring that other staff members use the information safely and responsibly. IAOs will be appointed based on sufficient seniority and level of responsibility and will be documented in our Information Asset Register (IAR).

2.5 ALL STAFF

All staff, including governors or trustees, contractors, agents and representatives, volunteers, and temporary staff working for or on our behalf, will be responsible for collecting, storing, and processing personal data in accordance with this policy.

3 DATA PROTECTION PRINCIPLES

We will comply with the data protection principles defined in Article 5 of the UK GDPR. We will ensure that personal information is:

- Processed lawfully, fairly and transparently **(Lawfulness, Fairness and Transparency)**.
- Collected only for specified, explicit, and legitimate purposes **(Purpose Limitation)**.

- Adequate, relevant, and limited to what is necessary for the purposes for which it is processed **(Data Minimisation)**.
- Accurate and, where necessary, kept up to date **(Accuracy)**.
- Not kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the data is processed **(Storage Limitation)**.
- Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage **(Security, Integrity and Confidentiality)**.

We recognise that we must comply with the above principles and be able to demonstrate our compliance **(Accountability).**

4 LAWFUL BASES

UK GDPR sets out several conditions for lawfully processing personal information. We will usually rely on the lawful basis of public task or legal obligation; however, we may sometimes rely on our legitimate interests. We will only do this where we use data in ways individuals would reasonably expect and where we have a justifiable reason.

When relying on our legitimate interests, we will ensure that we provide individuals with clear and transparent information about how personal data will be used, including details on how to opt-out.

We may rely on vital interests as the lawful basis for sharing information in a situation where we believe someone is at risk of serious harm, for example, in a mental health emergency.

We will have an Appropriate Policy Document (APD) in place (see Appendix One) that provides information about our processing of special category (SC) and criminal offence (CO) data and demonstrates how we comply with the requirements of the UK GDPR and DPA.

5 DATA SUBJECT RIGHTS

Under the UK GDPR, individuals have several rights in relation to the processing of their personal data:

5.1 RIGHT TO BE INFORMED

When we collect their data, we will provide individuals with privacy information, normally through a privacy notice made easily accessible to the data subject. Privacy notices will be clear and transparent, regularly reviewed, and include all information required by data protection legislation.

5.2 RIGHT OF ACCESS

Individuals have the right to access and receive a copy of the information we hold about them. This is commonly known as a subject access request (SAR). We will have a SAR procedure that details how we deal with these requests (Appendix Two).

Other rights include the right to rectification, right to erasure, right to restrict processing, right to object, right to data portability and rights related to automated decision-making, including profiling.

Requests exercising these rights can be made to any staff member. Still, we encourage requests to be made in writing, wherever possible, and forwarded to the DPT, who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from our DPO service where necessary.

A record of decisions made regarding the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision.

6 RECORDS OF PROCESSING

Under Article 30 of the UK GDPR, we must record our processing activities. We will do this by developing and maintaining an Information Asset Register (IAR), which will include, as a minimum:

- The organisation's name and contact details
- The name of the information asset
- The owner of that asset, known as the Information Asset Owner (IAO)
- The purposes of the processing
- A description of the categories of individuals and the types of personal data
- Who has access to the personal data, and who it is shared with
- The lawful basis for each processing activity
- The format and location of the personal data
- Details of any transfers to countries outside of the UK and the appropriate safeguards
- The retention periods for each asset
- A general description of the technical and organisational security measures to protect the information.

We review the IAR at least annually to ensure it remains accurate and up to date, consulting with the DPO service as necessary.

7 PRIVACY BY DESIGN AND RISK ASSESSMENTS

We will adopt privacy by design and implement appropriate technical and organisational security measures to demonstrate how we will integrate data protection into our processing activities.

We will conduct a data protection impact assessment (DPIA) when undertaking new, high-risk processing or making significant changes to existing data processing. The DPIA will consider and

document the risks associated with a project before its implementation, ensuring data protection is embedded by design and default.

The data protection principles will be assessed to identify specific risks. These risks will be evaluated, and solutions to mitigate or eliminate them will be considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, we will opt to do this.

8 INFORMATION SHARING

Sometimes, we must share information with third parties to effectively fulfil our duty of education provision. Our privacy notices and IAR will document routine and regular information-sharing arrangements.

Any further or ad-hoc information sharing will only be done in compliance with legislative requirements, including the ICO's data-sharing code of practice. We will only share personal information where we have a lawful basis, ensuring any disclosure is necessary and proportionate. All disclosures will be approved by the relevant staff member and recorded in a disclosure log.

9 CONTRACT MANAGEMENT

All third-party providers who process data on our behalf must be able to provide assurances that they have adequate data protection controls in place. Where personal data is being processed, we will ensure that a written contract includes all the mandatory data processing clauses in accordance with Article 28 of the UK GDPR.

We will maintain a record of our data processors and regularly review the data processing contracts, with support from the DPO service, to ensure continued compliance.

Where possible, personal information we process is not transferred outside of the European Economic Area (EEA), which the UK government deems to have adequate data protection standards. If personal data is transferred outside the EEA, we will consult with the DPO service and take reasonable steps to ensure appropriate safeguards are in place. These safeguards will be recorded in our data processor register.

10 TRAINING

We will ensure that appropriate guidance and training on data protection and access to information are given to our workforce, governors or trustees, and other authorised users. Training will be delivered as part of the induction process and at least every two years. Refresher training will be carried out as required.

Specialised roles or functions with key data protection responsibilities, such as the SIRO, DPT and IAOs, will also receive additional training specific to their role.

We will maintain a record of all completed training and ensure that data protection awareness is raised in staff briefings and through routine staff emails where appropriate.

11 DATA PROTECTION COMPLAINTS

Any complaints or concerns about our compliance with data protection legislation or how we have handled personal data will be dealt with as a data protection complaint or internal review request. Details of the process will be provided as part of the acknowledgement.

If an individual remains dissatisfied after we have concluded our internal process, they may complain to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods to report, enquire, register, and raise complaints are available on the ICO's website here.

APPENDIX ONE – APPROPRIATE POLICY DOCUMENT (APD)

1.1 INTRODUCTION

Bradford Academy Trust processes special category and criminal conviction data while fulfilling its functions. Schedule 1 of the Data Protection Act 2018 requires data controllers to have an 'appropriate policy document' where certain processing conditions apply for special categories of personal and criminal conviction data. This document will fulfil this requirement.

This will complement our existing records of processing as required by Article 30 of the UK General Data Protection Regulation. It will also reinforce our existing retention and security policies, procedures, and other documentation regarding special category data.

1.2 WE WILL PROCESS THE FOLLOWING SPECIAL CATEGORIES (SC) OF DATA:

- racial or ethnic origin
- religious or philosophical beliefs
- trade union membership
- health or medical information
- sex life and sexual orientation
- political opinions

We will also process criminal offence (CO) data under Article 10 of the UK GDPR, including pre-employment checks and employee declarations, in accordance with their contractual obligations.

We will rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to process special category and criminal convictions data lawfully:

1.2.1 ARTICLE 9(2)(A) – EXPLICIT CONSENT

We will ensure that consent obtained from individuals is clear and specific for one or more outlined purposes. It must be granted through affirmative action and recorded as a requirement for processing. We will also conduct regular reviews of consents to ensure they remain current and valid.

Ean example of such processing include asking visitors for health or medical information to aid them in an emergency.

1.2.2 ARTICLE 9(2)(B) – EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION

We must collect special category data to comply with our legal requirements as an employer and safeguard our pupils.

Examples include carrying out DBS checks on staff to evidence suitability for a role, collecting medical information to make reasonable adjustments at work and monitor staff absence, and keeping records of an employee's trade union membership.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we will rely on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection.**

1.2.3 Article 9(2)(c) – vital interest

We must share SC data where an individual is physically or legally unable to consent and there is a serious risk to life.

An example is when there is an urgent or emergency situation, and an individual is at risk of harm to themselves or to others, such as in a mental health crisis.

A Schedule 1 condition is not required for processing under Article 9(2)(c).

1.2.4 Article 9(2)(g) – reasons of substantial public interest

Much of our processing of SC data will be done so for the purposes of substantial public interest.

Examples include processing SC data to identify pupils who require additional support, such as special educational needs, processing safeguarding concerns to ensure the safety and well-being of pupils, or collecting medical information when monitoring pupil attendance and allergen or dietary requirements.

When processing data under Article 9(2)(g), we also require a Schedule 1 condition under the Data Protection Act 2018. The conditions we will rely on for this processing are **Schedule 1, Part 2, (6) – statutory and government purposes; (10) – preventing or detecting unlawful acts; and (18) – safeguarding of children and of individuals at risk.**

1.3 COMPLIANCE WITH DATA PROTECTION PRINCIPLES

We will have several policies and procedures in place to ensure our compliance with the Article 5 data protection principles and meet our accountability obligations:

1.3.1 Accountability principle

We will implement appropriate technical and organisational security measures to meet the accountability requirements. These will include:

- The appointment of a Data Protection Officer.
- Taking a data protection by design and default approach to our processing activities, including completing risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing an information governance framework.
- Ensuring we have compliant contracts in place with data processors.
- Implementing appropriate security measures regarding the personal data we process. Our Information Security Policy provides more detail.

1.3.2 Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. We will identify an appropriate Article 6 condition and, where processing SC or CO data, an Article 9 and Schedule 1 condition.

We will consider how processing may affect individuals concerned and provide clear and transparent information about why we process personal data, including our lawful bases, in our privacy notices and this document. All privacy notices will provide details of data subject rights. Our privacy information will be regularly reviewed and updated to reflect our processing accurately.

1.3.3 Principle (b): purpose limitation

Organisations can only act in ways and for purposes for which they are empowered to do so by law. Personal data is, therefore, only processed to allow us to carry out the necessary functions and services we are required to provide in line with legislation.

We will clearly set out our purposes for processing in our privacy notices, policies and procedures, and in our IAR. If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we will check that it is compatible with our original purpose, or we will advise individuals of the new purpose.

1.3.4 Principle (c): data minimisation

We will only collect the minimum personal data needed for the relevant purposes, ensuring it is necessary and proportionate. Any personal information no longer required, especially with special category data, will be anonymised or erased. Further information can be found in our Records Management Policy.

1.3.5 Principle (d): accuracy

When we become aware that personal data is inaccurate or outdated, we will take reasonable steps to ensure that data is erased or rectified without delay. Where we cannot erase or rectify the data, for example, because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision.

Where we have shared information with a third party, we will take reasonable steps to inform them of the inaccuracies and rectification. We will maintain a log of all data rights requests and have appropriate processes for handling such requests.

1.3.6 Principle (e): storage limitation

Our retention policy will set out how long we will retain records. Where there is no legislative or best practice guidance, the **SIRO** or **DPT** will decide how long the information should be retained based on its necessity for legitimate purposes. We will also maintain a destruction log, documenting and overview of the information that was destroyed, the date it was destroyed, and why. Further information can be found in our Records Management Policy.

1.3.7 Principle (f): integrity and confidentiality (security)

We will employ various technical and organisational security measures to protect the personal and special category data that we process. A full description of security measures can be found in our Information Security Policy.

In the event of a personal data breach, the incident will be recorded on a log, investigated, and reported to our DPO service where necessary. This process is documented in greater detail in our Information Security Policy.

APPENDIX TWO – SUBJECT ACCESS REQUESTS (SAR)

Under the UK GDPR, individuals have the right to make a subject access request (SAR) to any member of our workforce, governor or trustee, contractor or agent working on our behalf. Requests need not be made in writing, but we will encourage applicants to do so where possible. Requests should be logged on our Data Protection form located on the Staff Dashboard or forwarded to the DPT who will log and acknowledge them within five working days.

We must be satisfied with the requestor's identity and may have to ask for additional information to verify this, such as:

- valid photo ID, such as driver's licence or passport
- proof of address, such as a utility bill or council tax letter
- confirmation of email address.

Only once we are confident of the requestor's identity and have sufficient information to understand the request will it be considered valid. We will then respond to the request within the statutory timescale of one calendar month.

If the request is considered 'complex', we can apply a discretionary extension of up to two more calendar months. If we wish to apply an extension, we will inform the applicant within the first calendar month of receiving the request.

Requests are considered 'complex' only if we can demonstrate that they meet one or more of the following factors:

- Information is technically difficult to retrieve, or specialist support is required.
- Large volumes of sensitive information where exemptions may need to be applied.
- Clarifying potential issues concerning confidentiality and/or disclosure of sensitive information.
- Needing to obtain specialist legal advice.
- Searching large volumes of unstructured manual records.

Requests involving large volumes of information may add complexity, but volume alone is not considered 'complex.'

If we consider applying exemptions to the requested information before disclosure, we will seek guidance from our DPO service. We may also refuse a manifestly unreasonable or excessive request in limited circumstances.

If a parent whose child is 12 years or over makes a subject access request, we may consult with the child, ask that they submit the request on their own behalf, or confirm permission for the disclosure. This decision will be made based on the pupil's capacity to understand the request and disclosure risks.

Parents or individuals with parental authority requesting information about a pupil's education record will be handled under the Education (Pupil Information) (England) Regulations 2005 and responded to within 15 school days. Any charges that arise from this request will be applied at our discretion.

1 INTERNAL REVIEW

Complaints in relation to SARs will be processed as an internal review request.

An internal review will be handled by an appropriate staff member who was not involved in the original request. They will examine the original request and response and decide whether it was handled appropriately and followed the legislation. The reviewing officer will decide whether to uphold or overturn any exemptions. Where possible, a full response will be provided within one calendar month.

If an individual remains dissatisfied after our investigation, they may appeal to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods to report, enquire, register, and raise complaints are available on the ICO's website here.

APPENDIX THREE – FOI AND EIR REQUESTS

1 FREEDOM OF INFORMATION (FOI)

The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness and transparency in the public sector. It enables members of the public to scrutinise the decisions of public authorities more closely and ensure that services are delivered properly and efficiently. Public authorities have two main responsibilities under the Freedom of Information Act:

- To publish certain information about its activities in a publication scheme, and
- To process and respond to individual requests for information, with a duty to provide advice and assistance.

Under FOI, anyone can request access to the recorded information we hold. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. A code of practice under section 45 of the Act sets out recommendations for handling requests for information. To comply with this code, requests must:

- Be in writing
- Provide the name or company name and contact or email address
- Describe the information being requested
- Ideally, state the preferred format they would like the information to be provided.

Any request that cannot be answered promptly as part of normal day-to-day business or where we are asked to handle it under Freedom of Information will be treated as an FOI request.

Information can be withheld if one or more of the 24 exemptions within the FOIA apply. This could mean that certain information is not released in response to a request or is not published. Requests for information can be refused for reasons including:

- The information is not held
- It would cost too much or take too much staff time to comply with the request
- The request is considered vexatious
- The request repeats a previous request from the same person.
-

2 ENVIRONMENTAL INFORMATION REGULATIONS (EIR)

Requests for information related to the environment, including activities that may affect the environment, will be handled under the Environmental Information Regulations 2004. EIR is similar to FOI, but there is an even greater presumption of disclosure and fewer exceptions under which a request can be refused. Requests under EIR can also be given verbally and do not need to be in writing, but must include:

- A name or company name and contact or email address

- A description of the information being requested
- Ideally, state the preferred format they would like the information to be provided.

'Environmental information' includes information which relates to:

- the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites, including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements
- factors such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a)
- measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b), as well as measures or activities designed to protect those elements
- reports on the implementation of environmental legislation
- cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c)
- the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

3 REQUESTS FOR INFORMATION UNDER FOI AND EIR

Any requests received should be forwarded to the DPT, who will log the request and acknowledge it within five school days.

The DPT is responsible for:

- Deciding whether the requested information is held
- Locating, retrieving or extracting the information
- Considering whether any exemption or exception might apply and the balance of the public interest test and/or adverse effect test
- Preparing the material for disclosure and drafting the response
- Seeking any necessary approval for the response
- Sending the response to the requester.

FOI requests must be made in writing. We will only consider requests that provide a valid name and address and will not consider requests that ask us to click on electronic links. EIR requests can be made verbally; however, we will endeavour to follow up in writing with the requestor to ensure accuracy.

The SIRO and DPT will consider all requests where a public interest test is applied or where there is any doubt on whether an exemption or exception should be applied. In applying the public interest test, they will:

- Document clearly the benefits of both disclosing or withholding the requested information
- Where necessary, seek guidance from the DPO service and previous case law to decide where the balance lies.

We will adopt a model publication scheme and publish as much information as possible on our website to ensure transparency and accountability.

We will charge for supplying information at our discretion, per current regulations. If a charge applies, the applicant will receive written notice, and payment must be made before the information is supplied.

We will respond to requests within the statutory timeframes of 20 school days for FOI requests and 20 working days for EIR requests.

4 INTERNAL REVIEWS

Complaints regarding FOI and EIR will be processed as an internal review request and should be made within 40 working days of the applicant receiving the original response. After that time, we will not be obliged to respond to the request for a review.

An internal review will be handled by an appropriate member of staff who was not involved in the original request. They will examine the original request and the response sent and decide whether it was handled appropriately, according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn the decision to withhold information. A full response will be provided within 20 school days.

If an individual remains dissatisfied after we have concluded our internal review, they may appeal to the Information Commissioner's Office. Its contact details are below:

The telephone helpline (0303 123 1113) is open Monday to Friday between 9 a.m. and 5 p.m. (excluding bank holidays). Alternative methods to report, enquire, register, and raise complaints are available on the ICO's website here.

APPENDIX FOUR – CCTV SURVEILLANCE

This guidance aims to set out the Academy's approach to the operation, management and usage of closed-circuit television (CCTV) systems on school property.

1 STATEMENT OF INTENT

The purpose of the CCTV system is to:

- Protect the safety and wellbeing of pupils, our workforce and visitors.
- Protect members of the school community from harm to themselves or to their property
- Deter and discourage anti-social behaviour such as bullying, theft, and vandalism
- Protect school assets and buildings
- Support the police in the prevention or detection of crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- Monitor compliance with our rules, codes of conduct and policies.

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and the UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2 RELEVANT LEGISLATION AND GUIDANCE

This policy is based on:

2.1.1 LEGISLATION

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- 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 School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.1.2 GUIDANCE

- Surveillance Camera Code of Practice (2021)

2.1.3 DEFINITIONS

- Surveillance: the act of watching a person or a place.
- CCTV: closed circuit television; video cameras used for surveillance.
- Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance.

3 COVERT SURVEILLANCE

We will not operate covert surveillance technologies; therefore, this policy does not cover the use of such technology.

4 LOCATION OF THE CAMERAS

Transparency - The use of surveillance camera systems must be visibly signed. Signage will include the purpose of the system, the name of the organisation operating the system and details of who to contact about its use. The signage will be clear and unobstructed so that anyone entering the area knows they are being recorded.

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

- Secondary public school spaces including corridors, lobbies, dining spaces and reception areas
- Secondary pastoral restoration rooms
- Primary public school spaces including corridors, dining spaces and reception areas
- Primary Peace Room
- External spaces including coverage of car parks, playgrounds, sports fields and all other public accessible areas
- Sports Centre including fitness suite and public areas
- All Academy entrance and exit points.
- Academy school busses, both external and internal

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

Fixed cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

External vehicular cameras will only be used to assist in the resolution of any incidents that may occur.

5 ROLES AND RESPONSIBILITIES

5.1 THE GOVERNING BODY

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

5.2 THE EXECUTIVE PRINCIPAL

The executive principal will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection team to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure that all authorised individuals who access the CCTV system and its footage have completed comprehensive training provided by both the technical and data protection teams, covering proper system usage and ongoing compliance with data protection requirements.

- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the data protection team and having taken into account the result of a data protection impact assessment
- Decide, in consultation with the data protection team, whether to comply with disclosure of footage requests from third parties

5.3 The Data Protection Team

The data protection team will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system in line with data protection legislation.
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the UK GDPR and Data Protection Act 2018
- Monitor compliance with UK data protection law
- Act as a point of contact for communications from the Information Commissioner's Office (ICO)
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out annual checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

5.4 The Site Director

The Site Director will:

- Take care of the day-to-day maintenance and operation of the external CCTV system
- Liaise with the Academy's external CCTV monitoring service and take appropriate action where necessary
- Report any faults, issues or inaccurate date/time stamps in relation to external CCTV cameras with the external support provider / IT Director where necessary
- Liaise with the external support provider / IT Director to oversee the security of the external CCTV system and footage

5.5 The IT Director

The IT Director will:

- Take care of the day-to-day maintenance and operation of the internal CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly
- Work directly with the Site Director to ensure external CCTV systems are functional, secure and operational
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified

6 OPERATION OF THE CCTV SYSTEM

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system will not record audio except in specific locations:

- External Cameras
- Secondary Reception
- Primary Reception

Recordings will have date and time stamps. This will be checked by the IT Director termly and when the clocks change.

7 STORAGE OF CCTV FOOTAGE

Under Article 30 of the UK GDPR, we have a duty to ensure that all our data processing activities are recorded for accountability purposes. To fulfil this requirement, we maintain an Information Asset Register and ensure that the use of surveillance systems is detailed on it. Any external providers processing surveillance data on our behalf are included in our data processor register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and will be deleted in accordance with our retention schedule.

The Data Protection Team will carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period.

8 ACCESS TO CCTV SYSTEMS

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage. CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage. Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

Any individuals that access CCTV Recordings must record their name, the date and time, and the reason for access in the access log.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

9 ACCESS TO LIVE STREAMS, RECORDINGS AND REMOTE ACCESS

9.1 CCTV LIVE STREAMS

The following users will have access to view CCTV live streams only with the ability to review the previous 15 minutes of footage for clarification purposes:

- Primary Reception Kiosk – Primary gate camera
- John Craig Sports Centre Kiosk – Sports centre internal and external cameras

9.2 CCTV LIVE STREAMS AND RECORDINGS

The following staff roles have authorisation to access the CCTV live streams and recorded footage:

ROLE	SECONDARY	PRIMARY	EXTERNAL	SEMH	JOHN CRAIG SPORTS CENTRE
Executive Principal	X	X	X	X	X
Site Director	X	X	X	X	X
IT Director	X	X	X	X	X
AV / Media Technician*	X	X	X	X	X
Data Protection Team	X	X	X	X	X

ROLE	SECONDARY	PRIMARY	EXTERNAL	SEMH	JOHN CRAIG SPORTS CENTRE
Facilities team	X	X	X	X	X
Secondary Principal	X		X		X
Primary Principal		X	X		
Designated Safeguarding Lead	X	X			X
Assistant Principals**	X		X		X
SEMH Lead				X	
External Security Service			X		
John Craig Centre Staff***		X	X		X

* - For maintenance and support services only
** - Assistant Principal for Behaviour and Assistant Principal for Learning Culture
*** - To monitor lettings and activities taking place outside of school hours

Additional users may also be given temporary access at the discretion of the Executive Principal.

10 CCTV Remote Access

CCTV remote access to live streams will only be used for the for the purpose of pursuing the aims stated in section 1.1, particularly in relation to:

- Protecting the safety and wellbeing of pupils, our workforce and visitors.
- Protecting members of the school community from harm to themselves or to their property
- Detering and discouraging anti-social behaviour such as bullying, theft, and vandalism
- Protecting school assets and buildings

On this basis access will be limited to the following roles:

- Site Director
- IT Director
- Executive Principal
- External Security Service

11 SUBJECT ACCESS REQUESTS (SAR) IN RELATION TO CCTV FOOTAGE

An individual's request for surveillance data held about them will be treated as a subject access request (SAR). See Appendix Two. CCTV Footage that may identify other data subjects may need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out data subject's faces, or redacting parts of the footage. If this is not possible the school may, where appropriate consult with the individuals involved before disclosure. If permission is not forthcoming the still images may be released instead.

12 THIRD-PARTY ACCESS

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the Data Protection Team.

The school will comply with any court orders that grant access to the CCTV footage. Requests for surveillance data from an official agency, such as the police or insurance providers, will be processed as ad hoc disclosure requests. We will confirm the purpose of the request and the lawful basis for accessing the data. We may also require formal documentation in support of the request. If we have any concerns about such requests, we will liaise with our Data Protection Officer (DPO).

All requests for surveillance data will be recorded on a log detailing who made the request, the purpose, whether the information was disclosed or refused, and the authorising staff member.

13 DATA PROTECTION IMPACT ASSESSMENT (DPIA) IN RELATION TO CCTV

The school follows the principle of privacy by design. Privacy is considered during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate. In addition CCTV surveillance systems are reviewed annually to ensure they remain necessary, proportionate and effective.

The DPO service will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Data Protection Team.

Those whose privacy is most likely to be affected, including the school community and neighbouring residents will be assessed and consulted where necessary during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be carried out whenever significant upgrades are implemented or where new cameras are installed that change the scope of coverage or impact to an individual's privacy.

If any security risks are identified during the DPIA, the school will address them as soon as possible.

14 SECURITY

- The IT Director will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected, and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible or during a suitable maintenance window

APPENDIX FIVE – NON-CCTV SURVEILLANCE

1 INTRODUCTION

This section concerns our use of non-CCTV based surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation, statutory guidance, and relevant codes of practice. For information regarding CCTV surveillance please refer to Appendix Three.

2 DEFINITIONS OF NON-CCTV SURVEILLANCE

Surveillance is the close observation or monitoring of people's activities or by the collection and analysis of personal data, such as monitoring emails, phone calls, and internet browsing.

We will not operate covert surveillance technologies; therefore, this policy does not cover the use of such technology.

2.1 E-MONITORING

'E-monitoring' or 'digital monitoring' is when an organisation uses software to monitor a user's activity on an electronic device or network. We will deploy e-monitoring software on all Bradford Academy owned equipment and across our network, covering fixed and portable devices (PCs, laptops, and tablets), including guest devices connected to our network.

The software will monitor typed activity and the content visible on a user's screen to detect inappropriate use. Inappropriate use will be reported to designated staff within our organisation through a screenshot and other relevant technical details for further investigation. Staff, students and guests accessing our network are subject to this monitoring.

We operate e-safety monitoring software to:

- Safeguard our pupils and staff.
- Promote wellbeing and early intervention in high-risk incidents.
- Ensure appropriate use of our assets and resources.
- Monitor compliance with our rules and policies.

2.2 CALL RECORDING

We may record incoming and outgoing telephone calls:

- For quality monitoring and staff training purposes.
- For the efficient resolution of disputes and complaints.
- To assist with informal or formal investigations.
- As evidence of safeguarding concerns.

3 DATA PROTECTION BY DESIGN AND DEFAULT

Under the UK GDPR, we must consider and address privacy implications for data subjects when implementing new data processing systems. This is known as privacy by design. The usual method for assessing privacy risks to individuals is to carry out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly privacy intrusive. We will ensure that DPIAs are completed for any surveillance system and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if any substantive changes are made to our systems.

We are open and transparent about using non-CCTV based surveillance technology and identify whether we are a controller or joint controller of the information. Where we use external providers to process the data on our behalf, we will have a written contract meeting the requirements of Article 28 of the UK GDPR. We will only use providers who can ensure they have appropriate measures to safeguard the data.

4 TRANSPARENCY

Users will be informed of e-monitoring in relevant policies, newsletters, internal communications, and visual cues such as notifications on visitor registration screens.

We will ensure we are transparent about call recording by including an automatic message for inbound calls that plays before the call connects and states that calls will be recorded. If call recording was to be implemented, we will add information about call recording to our website on the Contact Us web page and include it in new pupil and employee starter packs.

Our privacy notices will include more detailed information about our use of non-CCTV surveillance technologies, including information about data subject rights.

5 ACCESS CONTROLS

Logs of e-monitoring systems intended to safeguard children will only be examined where there is reasonable cause to believe a child is at risk. Call recordings will be only accessed if it is deemed necessary to meet one of the purposes described above.

Each system will have proportionate access controls and a nominated Information Asset Owner (IAO) who will be responsible for its governance and security. The IAO may authorise other specified staff members to access data on the systems routinely or on an ad-hoc basis.

6 AD-HOC REQUESTS AND DISCLOSURES

An individual's request for non-CCTV based surveillance data held about them will be treated as a subject access request (SAR). See Appendix Two.

Requests for non-CCTV based surveillance data from an official agency, such as the police or insurance providers, will be processed as ad hoc disclosure requests. We will confirm the purpose of the request and the lawful basis for accessing the data. We may also require formal documentation in support of the request. If we have any concerns about such requests, we will liaise with our DPO service.

All requests for non-CCTV based surveillance data will be recorded on a log detailing who made the request, the purpose, whether the information was disclosed or refused, and the authorising staff member.

7 RECORDS OF PROCESSING AND RETENTION

Under Article 30 of the UK GDPR, we have a duty to ensure that all our data processing activities are recorded for accountability purposes. To fulfil this requirement, we maintain an Information Asset Register and ensure that the use of surveillance systems is detailed on it. Any external providers processing surveillance data on our behalf are included in our data processor register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and will be deleted in accordance with our retention schedule.

8 REVIEWS

Non-CCTV based Surveillance systems will be reviewed annually to ensure they remain necessary, proportionate and effective. We will update the DPIAs to reflect any changes in system use or data collection type. The relevant IAO is responsible for ensuring reviews are completed, and evidence of this is maintained.