

DATA PROTECTION POLICY

V1.1

December 2025

Table of Contents

1.0	Policy Statement	3
2.0	Scope and Purpose.....	3
3.0	Overarching Principles	3
3.1	Legal framework	3
3.2	Definition of data protection terms.....	4
3.3	Data protection principles	4
4.0	Responsibilities and Arrangements	4
4.1	Responsibilities and Accountability	4
4.2	Fair and transparent processing	6
4.3	Lawful processing.....	6
4.4	Disclosure and sharing of personal information.....	8
4.5	Individual Rights Requests	8
4.6	Data breaches	11
4.7	Data Protection by design and default.	11
4.8	Data security and storage of records.....	12
4.9	Images and videos.....	12
4.10	Video surveillance	13
4.11	Biometric data.....	13
5.0	Complaints	13
6.0	Review of Policy	13
	Appendix 1: Definitions.....	14

1.0 Policy Statement

At Beckfoot Trust, we are committed to protecting the personal data of our pupils, staff, parents, and all individuals whose information we process. As a responsible data controller, we ensure that all personal and special category data is collected, stored, and processed lawfully, fairly, and securely. Compliance with data protection laws is fundamental to our operations, and we uphold the highest standards to safeguard privacy and prevent unauthorised access or misuse of personal data.

Aligned with our vision to be remarkable in all that we do, we approach data protection with the same high aspirations, ensuring all members of our community feel safe and valued.

Every member of our workforce has a responsibility to uphold this policy, and any breach may result in disciplinary action. By embedding our values of integrity, accountability, and care, we ensure that our data protection practices reflect our commitment to the success and well-being of our pupils, staff, and families.

2.0 Scope and Purpose

This policy applies to all personal data processed by Beckfoot Trust, including data relating to pupils, staff, parents, trustees, volunteers, and any other individuals whose information we hold.

It relates to personal data held in any format, including electronic, paper-based, and other recorded media and it governs all types of data processing activities such as collection, storage, usage, sharing, and disposal.

Beckfoot Trust are registered as a Data Controller with the Information Commissioners Office (ICO), under the reference number ZA023846.

The purpose of this policy is to ensure that Beckfoot Trust, as a Data Controller, processes personal data lawfully, fairly, and transparently in accordance with legal requirements and best practices.

It is designed to protect the rights and privacy of individuals by ensuring the safe and responsible handling of personal data and it aims to embed data protection principles into all aspects of Beckfoot Trust's operations, ensuring full compliance with relevant laws and regulations, and to minimise risks associated with data breaches, unauthorised access, or misuse of personal information.

Ultimately, this policy supports Beckfoot Trust's commitment to being remarkable in all that it does by maintaining trust, integrity, and accountability in data management.

3.0 Overarching Principles

3.1 Legal framework

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

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act
- Freedom of Information Act
- The Privacy and Electronic Communications Regulations (PECR)

It also has due regard to guidance produced by the Information Commissioner's Office (ICO), Department of Education and the Information Records Management Society.

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

- Biometric Information Policy
- Child Protection and Safeguarding Policy
- Freedom of Information Policy
- Online Safety and IT Use Policy
- Video Surveillance Policy
- Data Breach Procedure
- Data Protection Impact Assessment Procedure
- Individual Rights Request Procedure
- Records Management and Retention Procedure
- Data Processor Due Diligence and Contract Procedure

3.2 Definition of data protection terms

Appendix 1 to this policy contains a list of key data protection definitions.

3.3 Data protection principles

Anyone processing personal data must comply with the data protection principles. These state that personal data must be:

- processed fairly, lawfully and transparently in relation to the data subject
- processed for specified, explicit and legitimate purposes and in a way which is not incompatible with those purposes
- adequate, relevant and not excessive for the purpose
- accurate and up to date
- not kept for any longer than is necessary for the purpose and
- processed securely using appropriate technical and organisational measures.

Personal Data must also be processed in line with the data subject's rights and not be transferred to people or organisations situated outside of the United Kingdom without adequate protection.

4.0 Responsibilities and Arrangements

4.1 Responsibilities and Accountability

4.1.1 The Trust Board

The Trust Board has overall responsibility for ensuring that Beckfoot Trust complies with all relevant data protection obligations. This responsibility is delegated to Beckfoot Trust's Audit and Risk Committee, which has oversight of compliance with these obligations.

4.1.2 The Data Protection Officer

The Data Protection Officer is responsible for:

- overseeing the implementation of this policy
- monitoring Beckfoot Trust's overall compliance with this policy and data protection law
- advising on the development of related policies, procedures and guidelines

- supporting with Data Protection Impact Assessments
- acting as a contact point for data subjects and the supervisory authority
- advising and supporting the schools to meet their data protection obligations
- responding to data protection complaints
- investigating personal data breaches
- responding to information requests.

Beckfoot Trust's DPO can be contacted at compliance@beckfoot.org.

4.1.3 Data Protection Leads

Each school has a Data Protection Lead responsible for the day-to-day data protection matters and is contactable directly through individual schools.

The Data Protection Leads are responsible for:

- liaising with the DPO to advise and support the schools to meet their data protection obligations
- maintaining all data protection procedures and associated documentation
- ensuring consistent approach to data protection across the schools
- arranging appropriate training and guidance to support staff in meeting their duties under data protection laws
- supporting the DPO in investigating and responding to personal data breaches and
- supporting the DPO in responding to information requests.

4.1.4 Headteachers

Headteachers are responsible for:

- providing day-to-day leadership on data protection issues within their schools
- ensuring all staff fulfil their duties around data protection and
- ensuring all their staff complete any training arranged by our Trust.

4.1.5 All staff

All staff are responsible for:

- processing personal data in accordance with this policy, any associated guidance and any supplementary procedures issued by Beckfoot Trust
- recording personal data accurately, in a timely manner using appropriate record management systems
- not sharing personal data with individuals, external agencies, suppliers, or other organisations, unless it is appropriate for their job role and approval has been given
- updating their HR portal in the Every system with any relevant changes to their own personal data, such as a change of address, other contact details, or emergency contact information
- fully participating in all data protection training arranged for them, including familiarising themselves with any updated guidance that is issued by our Trust
- cooperating with any reasonable request for involvement in compliance monitoring

- reporting any personal data breaches, as soon as they become aware of it, in accordance with the Data Breach Procedure
- notifying their Data Protection Lead if they have any concerns that this policy is not being followed
- notifying their Data Protection Lead if they receive a request from an individual to exercise their rights, in accordance with the Individual Rights Request Procedure.

4.2 Fair and transparent processing

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

Personal data will be processed fairly, and in a way that data subjects would reasonably expect. To be transparent, data subjects must be made aware of the following privacy information:

- identity and contact details of the Data Controller and DPO
- what personal data is being processed
- why the personal data is being processed
- what the lawful basis is for processing
- whether the personal data will be shared, and if so with whom
- whether the personal data will be transferred outside the United Kingdom and if so the safeguards in place
- the period for which the personal data will be stored
- the existence of the data subject's rights in relation to the processing of that personal data and
- the right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

Beckfoot Trust will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered.

4.3 Lawful processing

4.3.1 Lawful basis for personal data

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

- where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract
- where the processing is necessary to comply with a legal obligation that we are subject to, for example the Education Act
- where the processing is necessary to ensure the vital interests of the individual, for example to protect someone's life
- where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest
- where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects or

- where none of the above apply then we will seek the consent of the data subject to process their personal data.

4.3.2 Lawful basis for special category personal data

When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under the following legal grounds:

- where the processing is necessary for employment law purposes, for example in relation to sickness absence
- where the processing is necessary to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment
- where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities and
- where none of the above apply then we will seek explicit consent from the data subject to process their special category personal data.

4.3.3 Consent

Where none of the other lawful basis for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any personal data for any purpose.

There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

If consent is required, then the form of this consent must:

- inform the data subject of exactly what we intend to do with their personal data
- require them to positively confirm that they consent, for example we cannot ask them to opt-out rather than opt-in and
- inform the data subject of how they can withdraw their consent at any time.

Any consent must be freely given, which means that Beckfoot Trust cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

When pupils join a Beckfoot Trust school, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things.

In relation to processing personal data of all pupils under the age of 13 years old, we will seek consent from an individual with parental responsibility for that pupil.

When gaining consent of pupils who are 13 or over, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be sought from pupils who demonstrate a clear understanding of what they are agreeing to.

Consent may need to be refreshed where personal data needs to be processed for a different and incompatible purpose which was not disclosed when the consent was first considered by the data subject.

A record must always be kept of any consent, including how it was obtained and when.

4.4 Disclosure and sharing of personal information

Beckfoot Trust may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, Education and Skills Funding Agency (ESFA), Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

Beckfoot Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.

For further information relating to safeguarding data, please refer to Beckfoot Trust's Child Protection and Safeguarding Policy.

4.5 Individual Rights Requests

Individuals have the right to submit an Individual Rights Request to any part of Beckfoot Trust, it does not need to be directed to a specific person or contact point. However, where possible, requests should be submitted to the Data Protection Lead of the relevant school or the Data Protection Officer.

Upon receiving an Individual Rights Request, the Beckfoot Trust will follow its established Individual Rights Requests procedure to ensure compliance with data protection regulations.

4.5.1 The right to be informed

Data protection laws require Beckfoot Trust to provide privacy information to individuals at the time personal data is collected, or within one month if personal data is collected from another source.

Privacy notices will be issued as outlined below and are available on the Beckfoot Trust's website or upon request from the relevant school.

Beckfoot Trust adopt the DfE Model Privacy Notices for schools as the basis of our privacy notices and wherever possible will ensure that the privacy notice is written in a clear, plain manner.

Beckfoot Trust have the following privacy notices:

- **Student and Families Privacy Notice**, this privacy notice is also built into School Admission Forms, which are signed by the parent/carer (person with legal responsibility) and the student where relevant, upon entry to the school
- **Workforce Privacy Notice**, which is also issued with the contract documentation and
- **Recruitment Privacy Notice**, which is available for potential employees applying for a position within Beckfoot Trust.

4.5.2 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 (SAR) 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.

Responses to SARs shall normally be made within one calendar month of receipt, however this may be extended by up to 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.

4.5.3 The right to rectification

Data subjects have the right to have inaccurate personal data rectified or incomplete personal data completed, although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

4.5.4 The right to erasure

Data subjects have a right to have personal data about them held by Beckfoot Trust erased, however this only in the following circumstances:

- where the personal data is no longer necessary for the purpose for which it was originally collected
- when a data subject withdraws consent, which will apply only where Beckfoot Trust is relying on the individual's consent to the processing in the first place
- when a data subject objects to the processing and there is no overriding legitimate interest to continue that processing – see below in relation to the right to object
- where the processing of the personal data is otherwise unlawful
- when it is necessary to erase the personal data to comply with a legal obligation.

Beckfoot Trust is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- to exercise the right of freedom of expression or information
- to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
- for public health purposes in the public interest
- for archiving purposes in the public interest, research or statistical purposes or
- in relation to a legal claim.

If Beckfoot Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

4.5.5 The right to restrict processing

Data subjects right to restrict the processing of their personal data in certain circumstances. This means that a data subject can limit the way that Beckfoot Trust uses their data. This is an alternative to requesting the erasure of their data.

Beckfoot Trust must restrict the processing of personal data in the following circumstances:

- where a data subject contests the accuracy of their personal data, and we are verifying the accuracy of the data and considering the request

- where a data subject exercises their right to object, they also have a right to request we restrict processing while we consider their request
- where the processing is unlawful, and the data subject opposes erasure and requests restriction instead
- where it no longer needs the personal data, but the data subject has asked Beckfoot Trust to keep the personal data because they need it in order to establish, exercise or defend a legal claim.

If Beckfoot Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

4.5.6 The right to data portability

The right to data portability gives data subjects the right to receive personal data they have provided to Beckfoot Trust in a structured, commonly used and machine-readable format. It also gives them the right to request that Beckfoot Trust transmits this data directly to another controller.

The right to data portability only applies when:

- the lawful basis for processing the data is consent or for the performance of a contract; and
- when processing is carried out by automated means (i.e. excluding paper files).

4.5.7 The right to object

Data subjects have the right to object to the processing of their personal data in certain circumstances. Whether the right applies depends on Beckfoot Trust's purposes and the lawful basis for processing.

Data subjects have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals may also object if the processing is for:

- a task carried out in the public interest
- the exercise of official authority vested in us or
- legitimate interests (or those of a third party).

Beckfoot Trust does not use 'legitimate interest' as a lawful basis for processing where it is acting in its official capacity.

If Beckfoot Trust can demonstrate it has legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or the processing is necessary for the establishment, exercise or defence of legal claims, it is not necessary to cease processing.

4.5.8 Automated decision making and profiling

Data subjects have the right not to be subject to a decision when it is based on automated processing, e.g. profiling and it produces a legal effect or a similarly significant effect on the individual.

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

- ensuring processing is fair and transparent
- using appropriate mathematical or statistical procedures
- implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors and
- securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

4.6 Data breaches

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 Data Protection Lead for the relevant school or the Data Protection Officer.

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, 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 employees should follow the Beckfoot’s Trust Data Breach Management Procedure.

4.7 Data Protection by design and default.

4.7.1 Data Protection Impact Assessments

Beckfoot Trust will comply with the requirements of data protection laws in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

Beckfoot Trust will complete an assessment of any such proposed processing and has a template document which ensures that all relevant matters are considered.

The Data Protection Officer should be consulted as to whether a Data Protection Impact Assessment is required, and if so how to undertake that assessment.

Trust employees should follow the Beckfoot Trust’s Data Protection Impact Assessment (DPIA) Procedure.

4.7.2 Data Processor Due Diligence and Contracts

Beckfoot Trust requires all third-party processors handling personal data on its behalf to provide written confirmation of compliance with data protection laws and that they maintain adequate security measures.

Before any data is transferred, Beckfoot Trust conducts due diligence to ensure compliance. Contracts with processors align with data protection laws, explicitly outlining their obligations and the rights of Data Subjects.

Trust employees ensure due diligence and contract compliance by following Beckfoot Trust's Data Processor Due Diligence and Contracts procedure.

4.8 Data security and storage of records

Beckfoot Trust will obtain and maintain 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 or theft is identified, extra measures to secure data storage will be put in place.

Beckfoot Trust, 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.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

All data is managed in accordance with Beckfoot Trust's Records Management and Retention Procedure.

4.9 Images and videos

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Beckfoot Trust wants to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. Consent will be sought of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

Whenever a pupil begins their attendance at a Beckfoot Trust school they, or their parent/carers where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

Some lessons may be recorded for teacher training purposes, Beckfoot Trust is not required to obtain permission for this.

Where photos are taken of visitors within our schools using a secure digital sign-in system, we will not ask for any sensitive data, other than individuals name and car registration which we ask as part of health and safety requirements.

4.10 Video surveillance

Beckfoot Trust operates video surveillance systems across our sites. Please refer to Beckfoot Trust's Video Surveillance Policy.

4.11 Biometric data

Beckfoot Trust operates biometric recognition systems within some our schools for the purposes of payment of dinner monies. Please refer to Beckfoot Trust's Biometric Information Policy.

5.0 Complaints

- A complaint about a data protection response from our schools should be sent to the DPO (compliance@beckfoot.org)
- The DPO will acknowledge receipt of the complaint and will provide a response without undue delay.
- Complainants will be informed of their right to escalate unresolved data protection concerns to the Information Commissioner's Office (ICO).

6.0 Review of Policy

The Risk and Compliance Manager will review this policy as appropriate and at least on an annual basis.

Appendix 1: Definitions

Term	Definition
Biometric Data	Data about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system, and can include fingerprint data, hand shapes, features of the eye or information about a person's voice or handwriting.
Biometric Recognition System	A system that operates automatically (electronically) which: <ul style="list-style-type: none"> • obtains or records information about a person's physical or behavioural characteristics or features; and • compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system.
Data	Data is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	The identified, or identifiable, living individual whose personal data is processed.
Personal Data	Any data relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	A person or organisation that determines the purposes and the means of processing personal data. Beckfoot Trust is the data controller for all personal data, including that which is processed by its schools, and used to carry out its functions.
Data Users	Data users are those of our workforce, whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	A person or organisation, other than an employee of Beckfoot Trust or any of its schools, who processes personal data on behalf of the data controller.
Processing	Anything done to personal data, including collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be manual or automated.
Special Category Personal Data	Types of personal data that are more sensitive and so need more protection. It includes information about an individual's: <ul style="list-style-type: none"> • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetics • biometrics, where used for identification purposes

	<ul style="list-style-type: none">• physical or mental health and• sex life or sexual orientation.
Criminal Offence Data	Any personal data relating to the commission of, or proceedings for, any criminal offence committed or alleged to have been committed by a person.
Workforce	Includes, any individual employed by Beckfoot Trust such as staff and those who volunteer in any capacity including Trustees or LSC Members.