the beckmead trust

nurture • sustain • grow

Data Protection Policy

Approved on:	16 July 2026
Approved by:	Board of Trustees
Last reviewed on:	July 2026
Reviewed by:	Dee Fullerton
Next review due by:	July 2027

Summary of Changes

Date	Updates	Page No.
04/2026	• The previous policy required updating due to new legislation and responsibilities post 2023: • The Data (Use and Access) Act 2025 (DUAA) - amends UK GDPR to modernize data usage. Key changes for schools include • Consent & Processing: Consent is now the primary method for processing, with a list of derogated purposes for flexibility. • Legitimate Interests: A new "recognized legitimate interests" clause is introduced. • Research: Rules are clarified to facilitate data usage for scientific research. • Automated Decision-Making (ADM): Restrictions on ADM are lifted for non-special category data, allowing more AI-driven decisions. • Cookies & Marketing: Allows for easier cookie consent and allows charities to send, and certain organisations to send, direct marketing via email without consent in specific scenarios. • ICO Empowerment: The ICO gains new powers to compel witnesses, request technical reports, and issue higher fines (up to £17.5 million or 4% of global turnover under PECR). • International Data Transfers: UK organizations must now rely on the UK IDTA (International Data Transfer Agreement) or the new EU SCCs (Standard Contractual Clauses) for data transfers, notes BDO	

Contents

1. Aims

The Beckmead Trust, and all schools within the Trust, aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied. It requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Trust will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

The Beckmead Trust, including all schools within its network will be referred to as 'the Trust' throughout this policy,

3. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025 (DUAA)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR. The Trust has a separate CCTV Policy.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

This policy will be reviewed annually to reflect "evolving technology" and "unforeseen risks" as highlighted in the Trust Digital Policy.

It should be noted that the Education (Pupil Information) (England) Regulations 2005, does not apply to academies. Requesters are asked to submit a Subject Access Request.

In addition, this policy complies with our funding agreement and articles of association.

Linked Trust Policies:

Reference should also be made to the following linked policies that are related to this Data Protection Policy and are designed to protect personal data:-

- The Trust Digital Policy
- The Data Retention Policy
- The Trust Staff Code of Conduct
- The Trust Freedom of Information Policy
- The Trust CCTV Policy
- The Trust Data Breach Policy
- The Trust Complaints Policy

These policies are also designed to protect personal data and can be found at on the Trust Website or by emailing information@beckmeadtrust.org

4. Definitions

TERM	DEFINITION
Personal Data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.
Special categories of personal data & Data Relating to Criminal Convictions and Offences	Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sexuality Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
Data Subject	An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.
Data Controller	The organisation storing and controlling such information ie The Beckmead Trust or a Beckmead Trust School. is referred to as the Data Controller. Our Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The Trust is registered with the ICO under The Trust, as legally required.

Data Processor	A data processor is any person or organisation (like a company) that processes personal data on behalf of a data controller, following the controller's instructions for how to process that data. Examples include outsourced IT support, payroll providers, or cloud services that store and manage data for other businesses. Processors must protect the data and comply with the controller's instructions, while the controller bears more responsibility for deciding the purpose and means of the processing.
Processing	Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, storing, recording, retrieving, using, disseminating, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties. Processing can be automated or manual.
Automated Processing	Any form of automated processing of personal data consists of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. An example of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision-making is prohibited except in exceptional circumstances.
Data Protection Impact Assessment (DPIA)	DPIA's are a tool used to identify risks in data processing activities with a view to reducing them
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Pseudonym ised	The process by which personal data is processed in such a way that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.

5. When can the Trust Process Personal Data?

The UK GDPR is based on data protection principles that our Trust must comply with. This policy sets out how the Trust aims to comply with these principles.

Data Protection Principles

The Trust is responsible for and adheres to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the Trust must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Trust only collects, processes and shares personal data fairly and lawfully and for specified purposes.

The Trust must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

The Trust may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The Trust may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;

- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of
- health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The Trust identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Where criminal records data is processed, a lawful condition for processing that data is also identified and documented.

Consent

Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

In cases of processing special category data and explicit consent, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any manner that is incompatible with the legitimate purposes specified.

The Trust will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and will ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data. [Please refer to the School's Data Retention Policy for further guidance].

Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data.

The Trust will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. A record will be kept of all data archived or destroyed within each School or Directorate. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Trust's Data Retention Policy for further details about how the Trust retains and removes data

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

- In order to ensure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -
- Encryption;
- Pseudonymisation (this is where the Trusty/School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Trust follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Full details on the Trust's security measures are set out in the Trust's Digital Policy (ICT).

Sharing Personal Data

The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local

Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the Trust shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data Outside the UK

The Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

6. Data Subject's Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the Trust handles their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing). To withdraw consent to processing at any time;
(b) Receive certain information about the Trust's processing activities;
(c) Request access to their personal data that we hold (see "Subject Access Requests" at **Appendix 2**);
(d) Prevent our use of their personal data for marketing purposes;
(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
(f) Restrict processing in specific circumstances;
(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;
(i) Object to decisions based solely on automated processing;
(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
(l) Make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales https://ico.org.uk/global/contact-us/; and
(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request.

7. Direct Marketing

The Trust is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

8. Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction [Please refer to the School's Digital Policy for further details about our security processes);
- Not remove personal data or devices containing personal data from the Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not store personal information on local drives.

9. Accountability

The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The Trust have taken the following steps to ensure and document UK GDPR compliance:-

10. Data Protection Officer (DPO) Contact Details

Please find below details of the Trust's Data Protection Officer: -

Data Protection Officer(DPO): Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London WC1C 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

Should you have any questions about the UK GDPR, the operation of this policy or, if you have any concerns that this policy is not being, or has not been, followed, please contact The Director of Compliance (dpo@beckmeadtrust.org) in the first instance. If the matter remains unresolved or requires further escalation, please contact the Trust's DPO using the details provided above.

11. Personal Data Breaches

The Trust maintains a robust procedure for identifying, investigating, and reporting personal data breaches. We are legally required to report high-risk breaches to the Information Commissioner's Office (ICO) within 72 hours.

All staff must report any suspected breach immediately. Full procedural steps are set out in the Personal Data Breach Policy **(Appendix 1).**

12. Transparency and Privacy Notices

The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices [and/or fair processing notices] which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The Trust's privacy notices are tailored to suit the data subject and set out information about how the Trust uses their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR. This includes the identity of the Data Protection Officer, the Trust's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly (for example, from a third party or a publicly available source), where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and where relevant, be written in a form understandable by those defined as "children" under the UK GDPR.

13. Privacy by Design

The Trust adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing data protection impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities
- For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

14. Data Protection Impact Assessments (DPIAs)

In order to achieve a privacy by design approach, the Trust conducts DPIAs for any new high risk technologies or programmes being used by the Trust which could affect the processing of personal data. The School carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

15. Record Keeping

The Trust is required to keep full and accurate records of data processing activities. These records include: -

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the Trust's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

A record of all subject access requests shall be kept by individual schools

The Compliance Directorate will keep a central record of all subject access requests received. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

16. Automated Processing and AI/LLM Governance

Any high-risk automated decision-making or AI implementation is strictly prohibited without a documented Data Protection Impact Assessment (DPIA) and formal approval from the Data Protection Officer (DPO). Staff must ensure that all use of AI and automated processing aligns

with the regulatory principles, approval processes, and data protection safeguards defined in the Trusts Digital Policy (Section C).

17. Roles and responsibilities

This policy applies to **all staff** employed by our Trusts, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

17.1 Trust Board

The Beckmead Multi-Academy Trust (MAT) is a single legal entity and the central data controller for all academies within its network. Under ICO guidance their responsibility is for data protection compliance, records management and cyber security across all constituent schools. Therefore, the MAT corporate body determines the purposes and means of processing personal data and holds overall responsibility for UK GDPR compliance.

Responsibilities of the MAT as the data controller include:

- **Governance and Accountability:** Trusts must formally document information governance frameworks and assign explicit responsibilities at both the trust and academy levels.
- **Cyber Security and Access Control:** MATs are explicitly required to enforce appropriate technical measures, including MAT-wide **Multi-Factor Authentication (MFA)** and robust password policies.
- **Subject Access Requests (SARs):** MATs must respond to SARs within one calendar month under UKGDPR.
- **Freedom of Information (FOI):** Adopt the ICO's Model Publication Scheme and publish a guide to information on their official websites.
- **Data Breach Reporting:** All personal data breaches must be logged. If a breach meets the threshold of risking individuals' rights and freedoms, it must be reported to the ICO without undue delay, and in any event, within **72 hours**.
- **Data Protection Officer (DPO) Oversight:** The ICO requires trusts to appoint an independent DPO to ensure there are no conflicts of interest across internal administrative staff.
- **Publishing Privacy Notices:** The trust must clearly explain how data is processed.

17.2 Governing Body

The governing board has overall responsibility for ensuring that their school complies with all relevant data protection obligations including the implementation of this policy.

17.3 Data Protection Officer

The Trust Data Protection Officer (DPO) is the first point of contact for individuals whose data the Trust processes, and for the ICO. The DPO will in turn liaise with the Director of Compliance in the first instance.

The Trust DPO is Judicium Data Services. Their contact details are noted in this policy at Section 10, page 15.

17.4. Director of Compliance

The Director of Compliance, supported by the DPO, is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies, procedures and guidelines where applicable. They will also be responsible for liaising with the Central IT Directorate for developing data relating policies and systems to support compliance.

They will provide an annual report of linked activities directly to Trustees and, where relevant advice and recommendations on Trust data protection issues. Termly reports will be provided to local Governing Bodies.

17.5 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis for individual schools. They will ensure their school follows the duties and guidelines set out in this policy to ensure compliance.

This includes forwarding any Subject Access Requests and notification of data breaches to the DPO immediately on receipt and responding to any related queries as a matter of urgency.

17.6 Beckmead Trust Central Executive Team

The Director of each individual directorate will act as the data controller representative for their directorate and will ensure their directorate follows the duties and guidelines set out in this policy to ensure compliance. This includes forwarding any Subject Access Requests and notification of data breaches to dpo@ beckmeadtrust.org immediately on receipt and responding to any queries relating to these as a matter of urgency.

17.7 Director of Data and Technology

The Director of Data and Technology will be responsible for updating the Beckmead Trust Digital Policy to reflect Trust needs, briefing the executive team, and providing oversight of digital implementation. This will include developing electronic systems and processes for implementation trust wide to maintain data protection compliance across the Trusts. This will include liaising with Trust Directorates and Headteachers as required.

17.8 All staff

All staff are required to familiarize themselves with this policy and comply with its provisions. For the purposes of this policy, 'staff' includes all employees, governors, trustees, and volunteers. Breaches of this policy may be dealt with under the Trust's Disciplinary Policy and Procedure up to and including dismissal depending on the seriousness of the breach.

Staff are responsible for storing and processing personal data in accordance with this policy, keeping data secure and ensuring their personal information held by the Trust is accurate. Staff must:

- Immediately report any suspected breaches or data queries
- Collect, store and process any personal data in accordance with this policy seeking advice from the Director of Compliance if:

    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Staff must comply with all training requirements related to this policy and also the Trust Digital Policy

18. Data Processors

The **data processors** are the external third-party organisations, IT platforms, and service providers
that process personal data on the trust's behalf and must strictly follow its instructions to ensure compliance with data protection law.

19. Collecting personal data

18.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. **Contract:**The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
2. **Legal Obligation:** The data needs to be processed so that the Trust can comply with a legal obligation. This includes processing required to comply with the law i.e. responding to the DfE returns or dealing with safeguarding queries.
3. **Vital Interests**: The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
4. **Public Task:** The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest or exercise its official authority ie covers core educational functions, statutory duties or delivering the curriculum.
5. **Legitimate Interests:** The data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
6. **Consent:** The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent. Also used for non-essential acts where individuals have a free choice is photography or marketing.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

18.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Data Retention Policy.

19. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

20. Subject Access Requests and other rights of individuals

Further information is detailed in **Appendix 2**

20.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing to and include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

20.2 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.

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 pupils at our Trust may be fufilled without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the Trust is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child

20.3 Responding to subject access requests

Procedures for handling Subject Access Requests, including timescales, verification of identity, and processing requests for children, are details in **Appendix 2.**
Reference should be made to this appendix by all parties when managing a SAR

20.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests

- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO (Section 9, page 15). If staff receive such a request, they must immediately forward it to the DPO (section 9 page 15).

21. Parental requests to see educational records

Parents, or those with parental responsibility, have a legal right to access to their child's educational record. Requests must be submitted by way of a Subject Access Request (SAR). If the request is for a copy of the educational record, the Trust may charge a fee to cover the cost of supplying it.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

Reasonable charges may be put forward for administration of educational records please email our DPO (Section 9, page 15) if you would like to make a request.

22. CCTV

We use CCTV in various locations around the Trust sites to ensure safety and security. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Please refer to the Trust CCTV Policy. Any other enquiries about the CCTV system should be directed to the (Director of compliance via dpo@beckmeadtrust.org).

23. Photographs and videos

As part of our Trust activities, we may take photographs and record images of individuals within our Trust.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at Trust 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 in advance.

If staff are included in photos or videos taken by parents/carers, their permission must be obtained before the material is circulated on social media or any other platform.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Where the Trust takes photographs and videos, uses may include:

- Within Trust on notice boards and in Trust magazines, brochures, newsletters, etc.
- Outside of Trust by external agencies such as the Trust photographer, newspapers, campaigns
- Online on our Trust website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

24. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use. The password lock will be used for electronic devices when the device is on and in use if the user is not at the machine for any period of time.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access. They must be kept secure at all times.
- Staff are prohibited leaving work devices or media unattended in public places or in sight in vehicles.
- Where personal information needs to be taken off site, staff must sign it in and out. Central Directorates will have their own separate log.
- All users of the trust/school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security

of their passwords and accounts. Staff or students who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked. Further details regarding the use of passwords can be found in the Trust Digital Policy.

- Any mobiles are used for work (e.g., emails) must be secured with a PIN or biometric lock.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see The Trust Digital Policy for further guidelines around acceptable and unacceptable use.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Data Security and Password Management

All staff must adhere to the password standards and technical security requirements defined in the
Trust Digital Policy (Section A8). This includes the mandatory use of Trust-approved password managers to store all credentials securely. The sharing of account or password information is strictly prohibited and constitutes a breach of this policy.

Further information around security of data can be found in the Trusts Digital Policy.

25. Disposal of 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.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Please refer to the Trust Data Retention Policy for further details.

26. Training

The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

All staff and governors are provided with data protection training as part of their induction process. General GDPR annual refresher training is mandatory for all staff.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.
To ensure robust data protection and cyber-security, all staff must complete annual mandatory
training modules. These modules must cover the specific areas identified in the Trust Digital Policy
(Section B11), including Social Engineering (methods used by hackers to trick people), Multi-factor Authentication (MFA), the risks associated with Removable Storage, and the procedures for
reporting personal data breaches or cyber incidents.

27. Audit

The Trust, [through the Director of Compliance working with the DPO will regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place regularly in order to review use of personal data.

28. Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate, at least annually.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.

29. Complaints relating to the use of your personal data

30. Mobile Phone Policy

All staff, pupils, and visitors must adhere to the protocols regarding the use of personal and work-issued devices as set out in the **Trust Digital Policy (Section D)**.

31. ICT Disaster Recovery

In the event of a significant data breach, system failure, or cyber-attack, the Trust follows the Disaster Recovery procedures outlined in the Trust Digital Policy (Section E).
If you believe your personal data has been mishandled, please submit a formal complaint by emailing information@beckmeadtrust.org. Complaints will be acknowledged within 30 days and handled in accordance with the Trust Complaints Policy. A standard complaint form is available in Appendix 5 for your convenience.

Appendix 1: Personal Data Breach Procedure

Please see the Trust Data Breach Policy. 24-26 Data Breach Policy.docx (Change to pdf)

Appendix 2 : Subject Access Request Procedure

Under Data Protection Law, data subjects have a general right to find out whether the Trust holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the Trust are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the Trust at potentially significant risk and so the Trust takes compliance with this policy very seriously.

A data subject has the right to be informed by the Trust of the following: -

(a) Confirmation that their data is being processed;
(b) Access to their personal data;
(c) A description of the information that is being processed;
(d) The purpose for which the information is being processed;
(e) The recipients/class of recipients to whom that information is or may be disclosed;
(f) Details of the School's sources of information obtained;
(g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, reliability and conduct; and
(h) Other supplementary information.

Timescale and Deadlines

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such a request as a matter of urgency.

Anyone within the Trust may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the Trust.

If you receive a SAR, please email our DPO via Judicium Data Services atdataservices@judicium.com.

A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording and it does not have to be on an official form. A SAR does not need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

How to Recognise a Subject Access Request
A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the Trust/ School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the Trust hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request
Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the Trust to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

I

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do When You Receive a Data Subject Access Request
All data subject access requests received should be immediately directed to dataservices@judicium.com who will review the request and what is required and liaise with the requester.

Subject Access Requests must be responded to within 1 month. This means there are limited timescales within which the Trust must respond to a request and any delay could result in failure to meet those timescales, potentially leading to enforcement action by the Information Commissioner's Office (ICO).

Acknowledging the Request
When receiving a SAR the DPO or Director of Compliance shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request. In addition to acknowledging the request, the DPO or Director of Compliance may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;
- if it is not clear where the information shall be sent, the DPO or Director of Compliance must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The Director of Compliance will work with the Trust and the DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request
Before responding to a SAR, the Director of Compliance will liaise with the School and will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward.

In the event of a parent making a request on behalf of a child please this will be done with the school and sight of photographic ID.

The Trust is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the Trust has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a

passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the Trust may ask the requester for more information for the purpose of clarifying the request, but the requester
shall never be asked why the request has been made. The DPO shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the Trust will be unable to comply with the request if they do not receive the additional information.

The Trust also retains the right to query overly complex or burdensome requests in line with data protection principles to ensure requests are proportionate and reasonable and do not disproportionately impact the Trusts' essential public duties or operational effectiveness. Any requests deemed complex, excessive or not being proportionate or reasonable may exceed the initial 1 month time frame to complete. The requester will be informed of this at the earliest opportunity.

Requests Made by Third Parties or on Behalf of Children

The Trust needs to be satisfied that any third party making a SAR request is entitled to act on behalf of an individual. It is the third party's responsibility to provide evidence of this entitlement.

This might be a written authority to make the request or it might be a more general power of attorney. The Trust may also require proof of identity in certain circumstances.

If the Trust is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it will contact the third party to query this and obtain consent. If the data subject requests the information requested to be sent directly to them a written request will be needed. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject

access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data.

Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights then the Trust should usually respond directly to the child or seek their consent before releasing their information by way of a signed consent form.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the Trust will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The Trust may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee For Responding to a SAR

The Trust will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the Trust will inform the requester why this is considered to be the case and that the Trust will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the Trust is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

The period for response may be extended by a further two calendar months in relation to complex, disproportionate or excessive requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

The Trust may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the School will be closed. As a result, it is unlikely that your request will be able to be dealt with during this time. We
may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The Trust will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
  - to request that the Company rectifies, erases or restricts the processing of his personal data; or
  - to object to its processing;
  - to lodge a complaint with the ICO;
  - where the personal data has not been collected from the individual, any information available regarding the source of the data;
  - any automated decision we have taken together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the Trust are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the Trust have one month in which to respond the Trust is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the Trust is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The Trust is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

The personal data the Trust needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the Trust may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (such as CPOMS, MyConcern);
- MIS system (such as Arbor, Bromcom);
- occupational health records;
- pensions data;
- payroll data:
- share scheme information;
- insurance benefit information.

The Trust should search these systems using the individual's name, initials, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The Trust will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to

the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances the Trust may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention:

The Trust does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references:

The Trust do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the Trust receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual/referee (i.e., the person giving the reference), which means that the Trust must consider the rules regarding disclosure of third-party data set out above before disclosing the reference. This would be done by applying the rules for Protection of Third Parties - either seeking the referees consent or determining if it is reasonable to disclose the information without their consent

Legal professional privilege:

The Trust does not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting:

The Trust does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations:

The Trust does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The Trust can refuse to comply with a request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;
- To avoid obstructing an official or legal inquiry, investigation or procedure;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
- To protect public security;
- To protect national security;
- To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to the Director of Compliance who will make the decision on the Trust behalf following advice.

In the event that the Trust decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive the Trust can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the Trust needs to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The Trust do not need to comply with the request until the fee has been received

Appendix 2 – Subject Access Request Form

The Data Protection Act 2018 provides the data subject, with a right to receive a copy of the data/information we hold about them or to authorise someone to act on their behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We will require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your current address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1:

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

YOUR DETAILS:

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address & Postcode	
Phone Number	
Email address	

Section 2:
Please provide details of the data subject ie the person whose personal data is being requested

DATA SUBJECT:

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address & Postcode	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- Birth certificate
- Driving licence
- Passport
- An official letter to my address

Personal Information

If you only want to know what information is held in specific records or about a specific topic/category please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:
If you are, or have been employed by the Trust and are seeking personal information in relation to your employment please provide details of your staff number, Beckmead Trust School, department and dates of employment etc.

Details:

Section 3

Please complete this section of the form with details about the Data Subject.

If you are acting on behalf of someone else (i.e., the data subject) then please answer the questions below. (This includes parents/carers requesting data on behalf of their children)

If you are **NOT** the data subject, but an agent appointed on their behalf or a parent you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Fore names	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- Birth certificate
- Driving licence
- Passport
- An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- Letter of authority
- Child Consent Form directly signed by the data subject
- Lasting or Enduring Power of Attorney
- Evidence of parental responsibility
- Other (give details):

Section 4

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

Please indicate how you wish to receive this date

I wish to:

- Receive the information by post*
- Receive the information by email
- Collect the information in person
- View a copy of the information only
- Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: dataservices@judicium.com

Appendix 3 - Child Consent Form

Consent for Sharing Personal Data

Your full name_____

Beckmead School_____

All schools collect a lot of information about their pupils. You have rights for the data the school holds about you. Schools won't be able to share everything, but we will share as much as the law says we can.

We have received a request from your mother/father/guardian(delete as appropriate) who has asked for a copy of your data. We can only do this if you say we can.

Your consent

Please confirm how you would like us to handle your information by ticking the correct selection below. If you are not sure and feel you need further information of what this means before you make a decision please let us know.

□ I would like my data to be disclosed to the person detailed above.

OR

□ I would like my data to be disclosed directly to me.

OR

□ I do not want my data to be disclosed to the person detailed above or to me.

Your signature: _____

Your name: _____

Date: _____/_____/_____

Appendix 4 - Guide to making a SAR to Beckmead Trust Schools

Guidance - Making a SAR Request to a Beckmead School.pdf

Appendix 5: Complaints Handling Procedure & Form

All complaints relating to GDPR will be dealt with via our complaint policy. The Complaints Policy is available on the Trust website.

In order to process your complaint as quickly as possible it would be helpful if you could provide the following information:

1. **Details of Complaint**
    a. Nature of Data: (e.g., Pupil records, photographs, CCTV, health records).
    b. Incident Description: Please provide a detailed description of the incident, including dates, names of staff involved, and how the data was used, shared, or lost.
    c. Data Protection Issue: (e.g., Unauthorised access, improper sharing, inaccuracy, failure to fulfill a subject access request).

2. **Desired Outcome**
    What action would you like the school to take to resolve this issue? (e.g., Correct data, destroy data, provide access, stop processing).

3. **Supporting Evidence**
    Please attach any supporting documents or correspondence.

4. **Declaration**
    "I confirm that the information I have provided is accurate and I am the data subject (or representing them)."

5. Signature (or electronic acknowledgment): _____ Date: ____/____/____