The Bishop Wheeler Catholic Academy Trust

Policy

Data Protection

Published: September 2023

To be reviewed: 2025/26

The Bishop Wheeler Catholic Academy Trust

Our Mission

Outstanding Catholic education for all pupils. As a family of schools, we will enable our young people to develop spiritually, morally, intellectually and personally, putting their faith into action, through serving Christ in others, in the church and in the world around them.

This policy was approved by the Resources Committee on behalf of the Trust Board

Signature:

Mrs D Gaskin
Chair of Trust Board

Date: 26/09/23

Version		3.0	
Date		September 2023	
Approved by Resources Committee		26/09/23	
Version	**Date**	**Description**	**Revision Author/s**
1.0 Published	June 2018	Trust Policy	Giles Nightingale (COO)/ Darren Beardsley (CEO)/ Jemma Johnson
2.0 Published	September 2021	Trust Policy Review	Darren Beardsley (CEO)/ Giles Nightingale (COO)/ Jemma Johnson/ Trust Board/ Trust Solicitors
3.0 Published	September 2023	Trust Policy review	JJN (Head of Governance) DBY (CEO) GNE (COO)

Change review

Version	Date	Changes
1.0	June 2018	New Policy
2.0	September 2021	Review
3.0	June 2023	**Definitions** – added, processing, personal data and special category data **Introduction** – Change to add policies to refer to, formatting changed. **Title changes** - Head of Governance **Purpose** – Information added. **Data Controller** – information added **Roles and Responsibilities** - added **Data Collection** – GDPR principles added **Special Category Data** - updated **Data Security** – information added **Information Sharing** – information updated **CCTV and Photography** - information added **Biometric recognition systems** – information added **Data Breaches** – updated **Data Subject Rights** – updated **Subject Access Requests** – updated **Contractors, Supply staff, and Voluntary Staff** – information added

Data Protection Policy

Contents

Definitions

In this policy for Data Protection, unless the context otherwise requires, the following expressions shall have the following meanings:

BWCAT	The Bishop Wheeler Catholic Academy Trust.
Trust, we and our	Covers all of the schools within The Bishop Wheeler Catholic Academy Trust and The Bishop Wheeler Catholic Academy Trust Office.
Governing Body	The Directors of the Trust Board.
Academy Council	Governors elected or appointed to individual Academy Councils.
CEO	The Chief Executive Officer for the Trust.
DPO	Data Protection Officer
ICO	Information Commissioner's Office
GDPR	General Data Protection Regulation
Personal Data	Any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including: • name • identification number • location data • online identifier It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.
Sensitive personal data (special categories of personal data)	Personal data which is more sensitive and so requires greater protection. This includes: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data for the purpose of uniquely identifying a natural person (e.g. fingerprints, retina and iris patterns),

	• health – physical or mental • sex life or sexual orientation. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
Processing	Any action involving personal information, including obtaining, viewing, recording, copying, amending, adding, deleting, extracting, storing, disclosing, destroying or otherwise using information. Processing can be automated or manual.
Data subject	The identified or identifiable individual who is the subject of personal data or the person to whom the information relates.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Introduction

The Bishop Wheeler Catholic Academy Trust (BWCAT), is committed to data protection and takes its responsibilities very seriously.

This policy sets out the Trust's accountability and responsibility for compliance with data protection law. This policy should be read in conjunction with the following:

- Privacy Notice
- ICT Acceptable Use Policy
- Records management Policy
- Freedom of Information Policy and Freedom of Information Publication
- Subject Access request Guidance
- Any other relevant guidance document.

The Bishop Wheeler Catholic Academy Trust is registered as a Data Controller with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are available on the ICO's website. The person responsible for Data Protection and will act as the Data Protection Officer (DPO) for the Trust is:

Jemma Johnson

BWCAT Head of Governance

j.johnson@bwcat.org

Purpose

This policy is intended to ensure that personal data is dealt with correctly and securely and in accordance with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This policy is in place to ensure all staff, Governors and Directors are aware of their responsibilities and outlines how the Trust complies with the core principles of the UK GDPR.

All persons involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines. Failure to comply with this policy may result in disciplinary action.

Good data management can bring many benefits both to individuals and on a Trust level; efficiency of services, improved data safety, high quality data, enhanced reputation as data handler, and compliance with the law lessens any financial threat of fines.

Scope

Personal data means any information relating to an identified or identifiable living person (referred to as a 'data subject'); an identifiable 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, online

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

This policy applies to all personal data we collect, process and store regardless of the location, how that personal data is stored and processed, regardless of the data subject or where the information originated from.

The Policy applies to information in all forms including, but not limited to:

- Hard copy of documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information stored on portable computing devices including mobile phones, tablets, camera and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images, including CCTV footage.

All staff, Directors, Governors and others processing personal data on the Trust's behalf must read this policy.

Trust schools also have a duty to issue a Privacy Notice to pupils/parents/carers/staff which summarises the information held, why it is held and the other parties to whom it may be passed on.

This policy will be reviewed and revised in accordance with our data protection obligations. We may amend, update or supplement it from time to time and will issue an appropriate notification of that at the relevant time.

General information about the GDPR can be obtained from the Office of the Information Commissioner (website http://www.ico.gov.uk).

The Data Controller

The Trust is the Data Controller under the UK GDPR and will endeavour to ensure that all personal information is processed in compliance with this Policy and the principles of the UK GDPR. The Trust, on behalf of its schools, has a duty to be registered as Data Controller with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are then available on the ICO's website.

Roles and Responsibilities

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

The Trust Board

The Trust Board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

The Academy Council

The Academy Council will support their Academy in maintaining effective and efficient control of the management of data, and support the Trust in achieving compliance with data protection law. The Academy Council will also report any significant concerns that cannot be addressed by the Academy alone, and any proposals for development, through the appropriate channel to the Trust's senior executive officers and/or the Trust Board.

The Trust Head of Governance (DPO)

The Trust Head of Governance will act as the Data Protection Officer (DPO) for the Trust. The DPO is a statutory position and will operate in an advisory capacity. The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

Duties will include:

- Acting as the first point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the data asset register and information governance policies, including annual audits at each Academy.
- Monitoring compliance with this policy and other relevant data protection law
- Assisting with the reporting and investigation of information security breaches;
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and reporting to the Trust Board and CEO on the above matters.

Executive Headteacher/Headteacher and Chief Executive Officer

Executive Headteacher/Headteacher within each academy, and the Chief Executive Officer on behalf of the Trust office, will:

- Ensure that all staff have received appropriate GDPR and data protection training;
- Ensure all staff are aware of and understand this policy and associated policies and procedures;
- Encourage best practice information handling practices and
- Act as a data protection representative for the school

Staff responsibilities

Staff members who process personal data must comply with the requirements of this policy and all other relevant policies associated with data protection. Staff members must ensure that:

- All personal data is kept securely at all times both on and off site;

- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data is kept in accordance with the Trust's Record Management Policy;
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Executive Headteacher/Headteacher and the Trust Head of Governance;
- They participate in relevant data protection training;
- They read and seek to understand this and all other relevant policies, procedures and guidance documents;
- They support the Trust in achieving compliance with data protection law;
- Any data protection breaches (personal data or not) are immediately brought to the attention of the Executive Headteacher/Headteacher and the Trust Head of Governance and that they support the Head of Governance in resolving breaches;
- Where members of staff are responsible for supervising students or volunteers doing work which involves the processing of personal data, they must ensure that those persons are aware of this policy and adhere to it;
- Personal data is only shared with others only when it is legally appropriate to do so and
- They inform the Academy of any changes to their own personal data.

Data Collection

Lawfulness, fairness and transparency

BWCAT collects and uses personal information about staff, pupils, parents, governors, directors, volunteers, external students and other data subjects who come into contact with its academies or central team. This information is gathered in order to enable us to provide education and perform other associated functions. In addition, there is a legal requirement on us to collect and process information to ensure that the academies comply with their statutory obligations.

Personal data must only be collected for the original purpose it was collected. If personal data is processed for another reason, a new Privacy Notice will need to be issued.

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

- the data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract;

- the data needs to be processed so that the academy can **comply with a legal obligation;**

- the data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life;

- the data needs to be processed so that the academy, as a public authority, can perform a task **in the public interest,** and carry out its official functions;

- the data needs to be processed for the **legitimate interests** of the academy or a third party (provided the individual's rights and freedoms are not overridden);

- the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

We will:

- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices; and
- Where Special Category Data is processed, also identify a lawful special condition for processing that information and document it.

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 to do their jobs. 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 Records Management Policy and Records Retention Schedule.

The Trust will aim to ensure data held about pupils, parents/carers and staff is as accurate and up to date as reasonably possible. The Trust requests all data subjects to inform us of any changes to information held and offers frequent reminders to data subjects to do this.

The Trust will only gather and process data that it considers necessary to carry out its educational purposes effectively. It will ensure that data is not held any longer than is necessary and, once no longer needed, it is properly destroyed/erased. All data which is no longer necessary and should not be retained, must be destroyed in a secure and appropriate manner. All personal data which is destroyed must be logged on the Academy or Trust Office destruction log.

Special Category Data

Special Category Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

The Trust processes special category personal data including information about health, religion, trade union membership and ethnicity.

We will only process Special Category Data if we have a lawful basis for doing so as set out in paragraph above; and one of the following special conditions applies:

- The data subject has given explicit consent;

- The processing is necessary for the purposes of exercising the employment law rights or obligations of the Trust or of the data subject;
- The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
- The processing relates to personal data which are manifestly made public by the data subject;
- The processing is necessary for the establishment, exercise or defence of legal claims; or
- The processing is necessary for reasons of substantial public interest.

For the purpose of data protection, the additional information that the Trust processes will also be treated as Special Category Data, due to its sensitivity:

- Details of relevant unspent convictions for the purposes of recruiting relevant staff;
- Checks conducted by the Disclosure and Barring Service for the purposes of assessing eligibility of staff or students to engage in work with children, as permitted by legislation relating to the rehabilitation of offenders or for determining fitness to practise relevant professions and
- Unspent convictions or allegations of sexual misconduct for staff and pupil disciplinary purposes.

Data Security

- All personal data regardless of the location and how it is stored and processed, must be kept secure at all times.
- Confidential paper records will be kept in a locked filing cabinet, drawer, or safe, with restricted access. Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data should be coded, encrypted, password protected or stored on the school system with the relevant security measures in place. Only person who are authorised should have access to individual files and folders.
- USB/Memory sticks must not be used.
- All electrical devices must be password-protected to protect the information on the device in case of theft.
- In order to be given authorised access to the computer network, staff and pupils will sign an Acceptable Use Agreement.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password. Emails that contain sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient, (information sent outside of the school/Trust).
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Computer printouts as well as source documents are shredded before disposal.
- Staff must 'lock' or close down computers when not in use.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas in BWCAT schools or the central Trust office containing sensitive information must be supervised at all times.

Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (displayed on individual Academy and the Trust websites). Information sharing agreements with third parties will be recorded on the Trust Data Asset Register (DAR).

The Trust will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the Trust will need to disclose data without explicit consent for that occasion. This is covered by the UK GDPR, Article 6 (1) (e), 'public task'.

These circumstances are largely but not exclusively limited to: -

- pupil data disclosed to authorised recipients, related to education and administration, necessary for the Trust to perform its statutory duties and obligations;
- pupil data disclosed to parents/carers in respect of their child's progress, achievements, attendance and behaviour;
- where there is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- staff data disclosed to relevant authorities e.g., in respect of payroll and administrative matters, such as HMRC;
- the prevention or detection of a crime and/or fraud or the apprehension or prosecution of offenders,
- as part of our safeguarding obligations. Our obligations to safeguarding and child protection are paramount. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.

Third party Data Processors

All third-party contractors who process data on behalf of the Trust must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

The Executive/Headteacher in each Academy may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the UK, then the Trust Head of Governance must be consulted prior to any contracts being agreed.

CCTV and photography

Recording images of identifiable individuals constitutes processing personal data, so such processing will be carried out in line with data protection principles and the Trust CCTV policy.

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.

BWCAT and its academies will always indicate its intentions for taking photographs of pupils and staff and will ask for consent before publishing them.

If BWCAT wishes to use images/video footage of pupils and staff in a publication, such as the Trust website, individual academy websites and prospectus, written consent will be sought for the particular usage.

Biometric recognition systems

Where we use pupils' or staff biometric data as part of an automated biometric recognition system, for example taking measurements from a fingerprint via a fingerprint scanner to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

The automated biometric recognition system will take measurements of a fingerprint and convert these measurements into a template to be stored on the system. An image of the fingerprint is not stored.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system. We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object.

Biometric data will be managed and retained in line with the Trusts Records Management Policy. Biometric data will be retained by the school for as long as consent is provided (and not withdrawn). Once a pupil or staff member leaves, the biometric data will be deleted from the school's system.

Biometric data will be kept securely and systems will be put in place to prevent any unauthorised or unlawful access/ use. The biometric data is only used for the purposes for which it was obtained and such data will not be unlawfully disclosed to third parties.

Data Breaches

The UK GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.

We will ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.

We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

The Trust's Data Breach Guidance and procedures must be adhered to at all times. Each Academy and the Trust Central Office must immediately report all data breaches to the Trust Head of Governance. Wherever possible the Trust Head of Governance will notify the ICO of any notifiable breaches within 72 hours of the breach occurring/being made aware of the breach.

Data Protection Impact Assessments (DPIAs)

Each Academy will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. The assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks.

The Trust Head of Governance will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the Trust Head of Governance will assist with the completion of the assessment, providing relevant advice.

Data Subject Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. The right to be **informed** - we will provide 'fair processing information', typically through a privacy notice.
2. The right of **access** – we will allow individuals to access their personal data so that they are aware of and can verify the lawfulness of the processing.
3. The right to **rectification** – we will ensure individuals entitlement to have personal data rectified if it is inaccurate or incomplete.
4. The right to **erasure** – we will meet the broad principle underpinning this right, of enabling an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances.
5. The right to **restrict processing -** in specific circumstances, permit individuals to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.
6. The right to **data portability** – we will allow individuals to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies: to personal data an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.
7. The right to **object** – we will permit individuals to object on "grounds relating to his or her particular situation". We will stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and

freedoms of the individual or the processing is for the establishment, exercise or defence of legal claims.

8. Rights in relation to **automated decision making and profiling** – we will identify whether any of our processing falls under Article 22 "Automated individual decision-making, including profiling" and, if so, make sure that we give individuals information about the processing; introduce simple ways for them to request human intervention or challenge a decision; carry out regular checks to make sure that our systems are working as intended.

Subject Access Requests

Individuals have the right to access their personal data that the Trust holds about them. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Under the GDPR, individuals have the right to obtain:

- confirmation that their personal data is being processed;
- access to a copy of their personal data (unless an exemption applies);
- 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;
- other supplementary information – this largely corresponds to the information that is provided in a privacy notice.

Requests for information should preferably be made in writing (including email), and be addressed to the Headteacher, to include:

• name of individual
• correspondence address
• contact number and email address
• details of the information requested

If the initial request does not clearly identify the information required, then further enquiries will be made.
If staff receive a subject access request in any form, then they must immediately forward it to the Headteacher. The Headteacher will correspondingly notify the Head of Governance.

Children and subject access requests
Personal data about a child belongs to that child, and not their 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. Pupils have a right of access under the UK GDPR to their own information.
The determination of whether a child can act for themselves is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request.

For any parent/carer request regarding a pupil the Headteacher may discuss the request with the pupil and take their views into account when making a decision. A pupil with competency to understand can refuse to consent to the request for their records. Where the pupil is not deemed to be competent to act for themselves in this regard, a parent or carer may make the decision on behalf of the pupil.

Responding to subject access requests

Any individual has the right of access to information held about them. The identity of the requestor must be established before the disclosure of any personal information, and it may be necessary to undertake checks regarding proof of relationship to the pupil.

The Trust may make a charge for the provision of information, dependent upon the following extracts from the UK GDPR:

- the school/Trust must provide a copy of the information free of charge. However, you can charge a
  'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The school/Trust must consult with the Head of Governance on any proposal to apply a 'reasonable fee'
- the school/Trust may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The school/Trust must consult with the Head of Governance on any proposal to apply a 'reasonable fee'
- the fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt of the request. However, this month will not commence until after receipt of fees or clarification of information sought. During school holiday periods we may extend the period of compliance, since the majority of staff are not contracted to work during the school holidays and access to information may not be possible.

We will be able to extend the period of compliance by a further two months where requests are complex, numerous or voluminous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where we process a large quantity of information about an individual, the UK GDPR permits us to ask individuals to specify the information the request relates to (Recital 63) and, although the UK GDPR does not include an exemption for requests that relate to large amounts of data, we are able to consider whether the request is manifestly unfounded or excessive.

We may not disclose information for a variety of reasons, such as if it:

- may cause serious harm to the physical or mental health or emotional condition of the individual, or another;

- would reveal that the pupil is being, or has been, abused or is at risk of abuse and where disclosure of that information would not be in the pupil's best interests;
- would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it;
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

Should we refuse to respond to a request, we will explain to the individual why, informing them of their right to complain to the ICO.

Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained to establish, if a complaint is made, what was redacted and why.

Data Transfer Outside the UK

Personal data can only be transferred out of the United Kingdom when there are safeguards in place to ensure an adequate level of protection for the data. Staff involved in transferring personal data either directly or indirectly through systems to other countries must ensure that an appropriate safeguard is in place before agreeing to any such transfer. This includes data on the internet as this can be accessed outside of the UK.

Advice should be sought from the Trust Head of Governance before personal data is transferred out of the UK.

Direct Marketing

We are subject to privacy laws and regulations under the Privacy and Electronic Communications Regulations 2003 (PECR). These regulations not only include rules regarding the direct marketing of the sale of products and services but also encompass the promotion of aims and ideals. Also applicable to Academies and the Trust is the governance of the promotion and notification of fundraising events and the selling of goods and services.

The law covers any means of electronic communications such as text, email, telephone and fax. Academies and the Trust must comply with this law at all times.

Academies are responsible for ensuring they are compliant with these laws, specifically around email marketing and that where appropriate, the regulations and guidance set out in PECR have been adhered to.

We will:

- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices; and
- Where Special Category Data is processed, also identify a lawful special condition for processing that information and document it.

Contractors, Supply staff, and Voluntary Staff

The Trust is responsible for the use made of personal data by anyone working on its behalf or on placement. Data Controllers should ensure that:

- Any personal data collected or processed in the course of work undertaken for or within the Trust is kept securely and confidentially;
- A copy of this policy is made available to the individual and is adhered to;
- All practical and reasonable steps are taken to ensure that contractors, supply staff or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

Data retention

Data will not be kept for longer than is necessary, and always in accordance with the Trust's published Records management Policy.

Data which is no longer required will be securely disposed of as soon as practicable.

Paper documents will be shredded or placed in confidential waste bins, and electronic data securely deleted, once the data should no longer be retained.

When archived personal data is destroyed the academy disposal log must be completed.

Complaints

Complaints in relation to Freedom of Information and Subject Access requests will be handled through our existing procedures and guidance. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the Trust Head of Governance.

If individuals are still not satisfied, you may also complain to the UK Information Commissioner's Office. Information on how to do this is available at http://ico.org.uk/complaints.

The 13 schools in our Trust:

St. Mary's Menston, a Catholic Voluntary Academy

St. Joseph's Catholic Primary School Otley, a Voluntary Academy

Ss Peter and Paul Catholic Primary School, a Voluntary Academy

Sacred Heart Catholic Primary School Ilkley, a Voluntary Academy

St Mary's Horsforth Catholic Voluntary Academy

St. Joseph's Catholic Primary School Pudsey, a Voluntary Academy

St Joseph's Catholic Primary School Harrogate, a Voluntary Academy

St Mary's Catholic Primary School Knaresborough, a Voluntary Academy

St. Stephen's Catholic Primary School and Nursery, a Voluntary Academy

Holy Name Catholic Voluntary Academy

St Roberts Catholic Primary School, a Voluntary Academy

St John Fisher Catholic High School Harrogate, a Voluntary Academy

St Joseph's Catholic Primary School Tadcaster, a Voluntary Academy

The Bishop Wheeler Catholic Academy Trust

The Bishop Wheeler Catholic Academy Trust is a charity and a company limited by Guarantee, registered in England and Wales.

Company Number: 8399801

Registered Office:

St. Mary's Menston,

A Catholic Voluntary Academy

Bradford Road

Menston, LS29 6AE

Website: bishopwheelercatholicacademytrust.org

Tel: 01943 883000

Email: j.johnson@bwcat.org

Chair of the Trust Board: Mrs Diane Gaskin