The Bishop Wheeler
Catholic Academy Trust

Policy

Data Protection

Published: June 2018

To be reviewed: 2020-2021

The Bishop Wheeler
Catholic Academy Trust

Our Mission

The school communities of The Bishop Wheeler Catholic Academy Trust will work together in truth and love to provide the best possible opportunities for all our young people and their families.

Our mission is the provision, development and future safeguarding of a World Class Catholic Education where every child, member of staff and family matters

The schools, their governors and the trust directors will work together, based on the principle of subsidiarity, in faithfulness and humility, to provide an education where Christ and His values of respect, service, tolerance, dignity and forgiveness are at the heart of everything we do.

This policy was adopted by the Trust Board

Signature:

Mrs C Hyde
Chair of Trust Board

Date: 10 July 2018

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

For the purpose of this policy, 'Trust, we and our' covers all of the schools within BWCAT and the BWCAT trust office.

This policy sets out the Trust's accountability and responsibility for compliance with data protection law. This policy should be read in conjunction with our Privacy Notices, the ICT Acceptable Use for Staff Policy, the E-Safety Policy and 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.

Purpose

This policy is intended to ensure that personal data is dealt with correctly and securely and in accordance with General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA).

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.

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

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.

Data Collection

BWCAT collects and uses personal information about staff, pupils, parents, governors, volunteers, external students and other data subjects who come into contact with the school. 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 schools comply with 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.

The collection of personal data will meet the principles of GDPR as laid out in section 3.

Data Retention

Personal data must not be kept longer than is necessary for the purposes for which it was originally collected. All personal data must be retained in conjunction with the IRMS 2016_IRMS_Toolkit_for_Schools_v5_Master (or subsequent versions). All data which is no longer necessary and should not be retained, must be destroyed in a secure and appropriate manner. Personal data may be kept for longer than is necessary if it is anonymised. All personal data which is destroyed must be logged anonymously in school and Trust Offices.

Data Security

All personal data regardless of the location and how it is stored and processed, must be secure at all times. Respective policies, training and guidelines for securing data must be adhered to at all times. This also applies to data sharing.

Data Breaches

The Data Breach Guidance and procedures must be adhered to at all times. Each school must immediately report all personal data breaches to the Data Protection Officer (DPO). The DPO will notify the ICO of any notifiable breaches within 72 hours.

Data Subject Rights

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

1. Where the legal basis of our processing is Consent, to withdraw that Consent at any time;
2. To ask for access to the personal data that we hold;
3. To prevent our use of the personal data for direct marketing purposes;
4. To object to our processing of personal data in limited circumstances;
5. To ask us to erase personal data without delay:
    a. If it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    b. If the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
    c. If the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
    d. If the data subject has objected to our processing for direct marketing purposes;
    e. If the processing is unlawful.
6. To ask us to rectify inaccurate data or to complete incomplete data;
7. To restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
8. To ask us for a copy of the safeguards under which personal data is transferred outside of the EU;

9. The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the Trust; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
10. To prevent processing that is likely to cause damage or distress to the data subject or anyone else;
11. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
12. To make a complaint to the ICO; and
13. In limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another school to which the pupil is transferring) in a structured, commonly used and machine readable format.

Subject Access Requests and Freedom of Information Requests

Requests must be complied with, usually within one month of receipt for Subject Access Requests and 20 working days for Freedom of Information requests. You must immediately forward any Data Subject Access Request you receive to the Headteacher or DPO. The relevant Requests Guidance documents and FOI Policy must be followed.

Data Transfer Outside the EEA

Personal data can only be transferred out of the European Economic Area when there are safeguards in place to ensure an adequate level of protection for the data. For transfers of personal data to a receiving party in the United States of America, the Privacy Shield Agreement between the European Union and the United States of America provides sufficient protection. Before transferring data, the Privacy Shield website should be consulted to determine whether the receiving party is on the Privacy Shield List. 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 EEA.

All schools are responsible for performing checks on where their personal data is.

Direct Marketing

We are subject to privacy laws and regulations under the Privacy and Electronic Regulations 2003 (PECR). These regulations not only include rules regarding the direct marketing of the sale of products and services but also encompasses the promotion of aims and ideals. Also applicable to schools 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. Schools and the Trust must comply with this law at all times.

Schools are responsible for ensuring that 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.

1. Lawful basis for processing personal data

We will ensure that the processing of personal data meets one of the following conditions:

1.1. That the data subject has consented to the processing;
1.2. That the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

1.3. That the processing is necessary for compliance with a legal obligation to which the Trust is subject;
1.4. That the processing is necessary for the protection of the vital interests of the data subject or another natural person;
1.5. That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by the Trust; or
1.6. Where the Trust is not carrying out tasks as a public authority, that the processing is necessary for the purposes of the legitimate interests of the Trust or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

We will:

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

2. Special Category Data

Special Category Data are 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 process 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 1 above; and one of the following special conditions applies:

2.1. The data subject has given explicit consent;
2.2. The processing is necessary for the purposes of exercising the employment law rights or obligations of the Trust or of the data subject;
2.3. The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
2.4. The processing relates to personal data which are manifestly made public by the data subject;
2.5. The processing is necessary for the establishment, exercise or defence of legal claims; or
2.6. 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 in its sensitivity:

2.7. Details of relevant unspent convictions for the purposes of recruiting relevant staff;
2.8. 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
2.9. Unspent convictions or allegations of sexual misconduct for staff and pupil disciplinary purposes.

3. Data Protection Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. We will ensure that personal data shall be:

3.1. Processed lawfully, fairly and in a transparent manner;
3.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
3.4. Accurate and, where necessary, kept up to date;
3.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and
3.6. Processed in a manner that ensures appropriate security of the personal data.

4. Roles and responsibilities

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

4.1. The Trust Board

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

4.2 Data Protection Officer (DPO)

The DPO is responsible for:

b) Advising the Trust and its staff of its obligations under GDPR;
c) Monitoring compliance with this policy and other relevant data protection law;
d) The Trust's policies with respect to data protection;
e) Audit activities related to GDPR compliance and
f) Cooperating with and act as the contact point for the Information Commissioner's Office

4.3 Staff responsibilities (includes contracted staff and staff contracted to work and Governors)

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:

a) All personal data is kept securely at all times both on and off site;
b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
c) Personal data is kept in accordance with the Trust's retention guidance;
d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Headteacher or DPO;
e) They participate in relevant data protection training;
f) They read and seek to understand this and all other relevant policies, procedures and guidance documents;
g) They support the Trust in achieving compliance with data protection law;
h) Any data protection breaches (personal data or not) are immediately brought to the attention of the Headteacher and the DPO and that they support the DPO in resolving breaches;
i) 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;
j) Personal data is only shared with others only when it is legally appropriate to do so and
k) They inform the school of any changes to their own personal data.

4.4 Privacy by Design

Staff will have due regard for Privacy by Design and will also, where applicable, undertake a Data Privacy Impact assessment if they are:

a) Engaging in a new activity that may affect the privacy rights of individuals;
b) Building new IT systems for storing or accessing or processing personal data;
c) Developing policies or strategies that have privacy implications;
d) Embarking on a data sharing initiative;
e) Using data for new purposes;
f) Using automated processing including profiling or
g) Undertaking large scale processing of special category data.

4.5 Schools and Trust Office

Each school will:

a) Be transparent about the personal data it processes and, at the first point of data collection, inform data subjects why and their personal data information is being processed by making the relevant Privacy Notice available to them;
b) Check the quality and the accuracy of the personal data holds;
c) Ensure that data is not retained for longer than is necessary;
d) Delete or anonymise personal data when it is obsolete in accordance to the guidelines;
e) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
f) Immediately contact the DPO to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests and Freedom of Information requests;
g) Immediately inform the DPO of any data breaches and follow breach procedures. Where there is doubt, contact must still be made;
h) Put the Data Protection Policy and Privacy Notices on their school website;
i) Where consent may be relied upon as the lawful basis for processing data, ensure that the DPO is consulted before any action is taken in order for the consent to be compliant with legislation;
j) Where a school uses CCTV, have a CCTV policy that outlines the reasons for using it and ensures it complies with the relevant regulations;
k) Where we use legitimate interest for our lawful basis for processing personal data, perform a balancing test beforehand to ensure this is the most appropriate lawful basis and aligned with the guidance laid out in the Legitimate Interests Guidance and Checklist document.
l) Ensure that the rights of all data subjects are respected;
m) SARs, FOIs and Consent Logs are completed and kept up-to-date;
n) Ensure that they can demonstrate compliance with GDPR;
o) Test its systems and processes on an annual basis to ensure compliance.

4.6 Headteachers and Chief Operation Officer

Headteachers within each school and the Chief Operating Officer on behalf of the Trust office will:

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

4.7 **Third-Party Data Processors** (including all IT platforms, virtual learning environments and apps where personal data e.g. pupil name is stored)

Where external companies are used to process personal data on behalf of the Trust, responsibility for the security and appropriate use of that data remains with the Trust.

Where a third-party data processor is used:

a) A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
b) Reasonable steps must be taken that such security measures are in place;
c) A written 'contract' establishing what personal data will be processed and for what purpose must be set out;
d) A data processing agreement must be signed by both parties;
e) Documentation outlined in c and d above must be retained and a copy sent to the DPO.

4.8 Contractors, Short-Term, Supply staff, School Direct Students, interns and Voluntary Staff

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

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

The 10 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

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:	a.tindall@stmarysmenston.org
Chair of the Trust board:	Mrs C Hyde
Vice Chair of the Trust Board:	Mrs D Gaskin