Bosco Data Protection & GDPR Policy

For all schools in the Bosco Catholic Education Trust

This GDPR Policy has been approved and adopted by the Bosco Catholic Education Trust.

Approved:	For review:
July 2023	July 2025

Bosco Catholic Education Trust Mission Statement

The Bosco Catholic Education Trust (Bosco CET) is a Christ-centred family of Catholic academies, within the Diocese of Arundel and Brighton, working together as one body to provide an outstanding education for all. As Catholic schools, we endeavour to develop confident, compassionate and faithful young people. Through partnership, collaboration and mutual support, we seek to enable all those entrusted to our care to become the person God called them to be.

"Serve the Lord joyfully"

Introduction

This Policy sets out the manner in which personal data is processed fairly and lawfully. The Policy complies with the Data Protection Act 2018 (DPA).

Bosco CET collects and uses personal information in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

Bosco CET is a data controller and must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. Bosco CET must be able to demonstrate compliance. Failure to comply with the Principles exposes Bosco CET and staff to civil and criminal claims and possible financial penalties.

Details of Bosco CET 's purpose for holding and processing data can be viewed on the data protection register: https://ico.org.uk/esdwebpages/search

The Bosco CET registration number is **ZA245247**. This registration is renewed annually and updated as and when necessary.

Aim

This Policy will ensure:

- Bosco CET processes person data fairly and lawfully and in compliance with the Data Protection Principles.
- All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.
- That the data protection rights of those involved with the School community are safeguarded.
- Confidence in the School's ability to process data fairly and securely.

Scope

This Policy applies to:

1. Personal data of Bosco CET trustees, staff, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.
2. Personal data of members of the public.
3. The processing of personal data, both in manual form and on computer.

Definitions

Personal data – any information relating to an identified, or identifiable, individual. This may include the individual's name, ID number, location data, etc. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special Category Data – personal data which is more sensitive and required more protection
This includes:

- 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
- Sex life or sexual orientation

The Data Protection Principles

Bosco CET will ensure that personal data will be:

1. Processed fairly, lawfully and in a transparent manner.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Bosco CET will be able to demonstrate compliance with these principles.

Bosco CET will have in place a process for dealing with the exercise of the following rights by individuals in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record, where appropriate;
- to erasure;

- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including
- profiling.

SCHOOLS

Roles and Responsibilities

The Governing Body of the School and the Head Teacher are responsible for implementing good data protection practices and procedures within the School and for compliance with the Data Protection Principles. In turn, the Governing Body of the School and the Head Teacher report to the trustees of the Bosco CET

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

A designated member of Bosco CET staff, the Data Protection Officer (DPO), will have responsibility for all issues relating to the processing of personal data. The DPO will liaise with Headteachers and will report directly to the Chief Executive Officer (CEO) of Bosco CET.

The DPO will comply with responsibilities under the Data Protection Act 2018 and will deal with subject access requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Bosco CET Complaints Policy.

The Data Protection Officer is Sheryl Cardwell and can be contacted at dpo@shardbusinessservices.co.uk.

Data Security and Data Security Breach Management

All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.

Access to personal data should only be given to those who need access for the purpose of their duties.

All staff will comply with the Bosco CET Acceptable IT Use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT Use Policy.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.
Bosco CET and each School will have in place a data breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) by the DPO in compliance with the Data Protection Act 2018.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix A

Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure outlined in Appendix B.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an academy context may include, but are not limited to:

- a non-anonymised dataset being published on the website which shows the exam results of pupils eligible for pupil premium
- safeguarding information being made available to an unauthorized person
- the theft of a school laptop containing non-encrypted personal data

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy 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
- 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

Requests for access to personal data will be processed by the DPO. Records of all requests will be maintained. You will not be charged for access to this information, unless multiple copies are requested, or the request is found unfounded or excessive.

When we receive a subject access request, we may ask you to provide us with a form of identification. The DPO will comply with the statutory time limit of one calendar month for effecting disclosure in response to a SAR. In cases where requests are more complex, we may extend this deadline to three months. If so, the individual will be informed within a month of your request with the reason as to why.

There are some cases in which we may not disclose information if it:

- Might cause serious harm to the physical or mental health of a pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interest
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If a request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. If we refuse a request, we will inform the individual why and inform them of their right to complain to the ICO.

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 aged 12 and above are generally 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 Academy Trust may not be granted 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.

Sharing data with third parties and data processing undertaken on behalf of the School.

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where a third party undertakes data processing on behalf of the School e.g. by providing cloud-based systems or shredding services, the School will ensure that there is a written agreement requiring the data to be processed in accordance with the Data Protection Principles. The School must consult with the DPO before implementing such an arrangement.

Ensuring compliance

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read the Acceptable IT Use Policy.

The School advises students whose personal data is held, the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the School and Bosco CET websites.

The School also provides a Privacy Notice to staff which is available on the School and Bosco CET websites.

The School will ensure Privacy Notices contains the following information:

- Contact information for the Bosco Data Protection Officer
- Purpose of processing and legal basis.
- Retentions period.
- Whom we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

Photographs, Additional Personal Data and Consents

Where the School seeks consents for processing person data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

Appendix A

What staff must do:

- ☑ **DO** get the permission of your manager to take any confidential information home.
- ☑ **DO** transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
- ☑ **DO** use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.
- ☑ **DO** ensure that any information on USB memory sticks is securely deleted off the device or saved on a School shared drive.
- ☑ **DO** ensure that all paper-based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
- ☑ **DO** ensure that any confidential documents that are taken to your home are stored in a locked drawer.
- ☑ **DO** ensure that paper-based information and laptops are kept safe and close to hand when taken out of premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
- ☑ **DO** ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
- ☑ **DO** return the paper-based information to the School as soon as possible and file or dispose of it securely.
- ☑ **DO** report any loss of paper-based information or portable computer devices to your line manager immediately.
- ☑ **DO** ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
- ☑ **DO** ensure that when posting/emailing information that only the specific content required by the recipient is sent.
- ☑ **DO** use pseudonyms and anonymise personal data where possible.
- ☑ **DO** ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic usernames, such as 'Sysman' are disabled.

What staff must not do:

- ☒ **DO NOT** take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
- ☒ **DO NOT** unnecessarily copy other parties into e-mail correspondence.
- ☒ **DO NOT** e-mail documents to your own personal computer.
- ☒ **DO NOT** store work related documents on your home computer.
- ☒ **DO NOT** leave personal information unclaimed on any printer or fax machine.
- ☒ **DO NOT** leave personal information on your desk overnight, or if you are away from your desk in meetings.
- ☒ **DO NOT** leave documentation in vehicles overnight.
- ☒ **DO NOT** discuss case level issues at social events or in public places.
- ☒ **DO NOT** put confidential documents in non-confidential recycling bins.
- ☒ **DO NOT** print off reports with personal data (e.g., pupil data) unless absolutely necessary.
- ☒ **DO NOT** use unencrypted memory sticks or unencrypted laptops.

Appendix B

This procedure is based on guidance on personal data breaches produced by the ICO.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third-party data processors must notify the Data Protection Officer immediately.

Step 2: The DPO must notify the CEO immediately when notified of a breach.

Step 3: The DPO will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from staff members and any third-party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the DPO will assess the potential consequences of the breach. The DPO should consider;

- How could it affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The DPO must decide whether or not the breach must be reported to the ICO. Breaches must be considered on a case-by-case basis; however, a breach must be reported to the ICO if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation

- damage to reputation
- or any other significant economic or social disadvantage to the individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the ICO.

Step 6: The DPO will document the decision taken as to whether or not the ICO are notified of the breach. The school should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the ICO. The school should keep a record of breaches whether or not they are reported to the ICO. This record should include:

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach
- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 8: In cases where the breach must be reported to the ICO, the DPO (or another member of staff if they are not available) must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant page on the ICO's website.

Step 9: The DPO must decide whether or not the individual is affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any affects and the likelihood of them being affected must guide this decision-making process. If there is a high risk the DPO will notify, in writing, all potentially affected individuals. This notification will include:

- Contact details for the DPO
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 10: The DPO must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the school or the ICO.