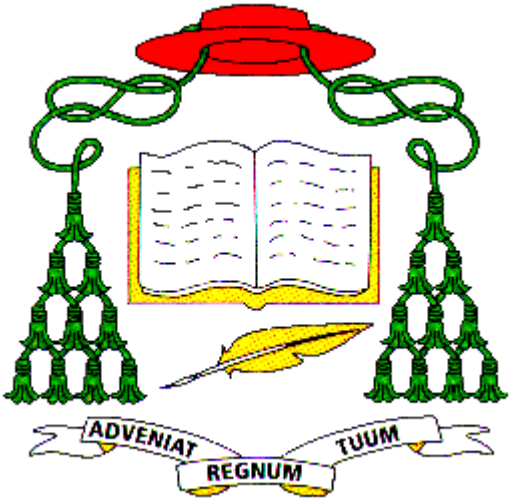

Archbishop Beck Catholic College

Data Protection Policy

Reviewed and Approved: December 2018

Renewal Date of Policy: December 2021

Our Commitment:

Archbishop Beck Catholic College is committed to the protection of all personal and sensitive date for which it holds responsibility as the Data Controller and the handling of such data is in line with the data protection principles, the Data Protection Act (DPA) and the General Data Protection Regulations.

Changes to data protection legislation will be monitored and implemented in order to remain compliance with requirements.

The member of staff responsible for data protection is Mr Phillips, Administration and Exams Manager (Data Protection Officer) supported by Leadership and Governors.

The college is also committed to ensuring staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the college and any third party contracted to provide services within the college.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and the ICO.

Personal and Sensitive Data

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. All data within the college's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protections/key-definitions.

The principles of the Data Protection Act shall be applied to all data processed:

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Processed fairly and lawfully;
2. Obtained only for one or more specified and lawful purposes and it not further used in any manner incompatible with those original purposes;
3. Accurate and where necessary, kept up to date;
4. Adequate, relevant and not excessive in relation to the purposes for which it is processed;
5. Not kept for longer than is necessary for those purposes;
6. Processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Protected by an appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage;
8. Not transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection of the personal information.

Fair Processing/Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation. https://ico.org/fororganisations/guide-to-data-protection/privacy-notices-transparency-and-control/.

The intention to share data relating to individuals to an organisation outside of our college shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact of an individual's privacy in holding data relevant to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements for any organization with which data is shared shall also be considered and these organization shall provide evidence of the competence in the security of shared data.

Individuals' Rights

The GDPR creates some new legal rights for individuals and strengthens some of the rights that currently exist under the Data Protection Act. These include:

1. The right to be informed
2. The right of access
3. The right of rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

1. Right to be informed

This is communicated through colleges' Fair Processing Notices/Privacy Notices and includes students, parents and staff. It is also available on the college website.

2. Right of Access

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 30 days and they should be made in writing to Mr Martin, College Business Manager (DPO).

3. Right of Rectification

All individuals have the right to have their data rectified if it is inaccurate or incomplete. If this rectified data has been share with 3rd parties they must be informed of the rectification where possible. Individuals must also be informed about the 3rd parties to whom the data has been disclosed where appropriate.

4. Right to Erasure

Also known as 'the right to be forgotten'. The individual is able to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This may be granted under specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processing in relation to the offer of information society services to a child.

5. Right to Restrict Processing

Individuals have the right to 'block' or suppress processing of personal data. When processing is restricted, we will store the data, but not further process it.

6. Right to Data Portability

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It can be copied, moved or transferred from one IT environment to another in a safe and secure way.

7. Right to Object

Individuals can object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority.
- Direct marking
- Processing for purposes of scientific/historical research and statistics.

8. Rights related to Automated Decision Making and Profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taking without human intervention. None of our systems constitute automated decision making.

Conflict of Interest

In the event that a conflict of interest occurs with the appointed DPO, a member of the Senior Leadership Team will take over any investigation/reporting in relation to the particular conflict.

Complaints

Complaints will be dealt with in accordance with the college's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Mr Phillips, Administration and Exams Manager/Data Protection Officer who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.