BISHOP CHALLONER CATHOLIC COLLEGE

DATA PROTECTION POLICY

INTRODUCTION

Bishop Challoner Catholic College is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the Data Protection Act. The school needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (eg to recruit and pay staff, to administer programmes of study, to record progress, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Any breach of the Data Protection Act 1998 or the Academy Data Protection Policy is considered to be an offence, and in that event school disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Academy, and who have access to personal information, will be expected to read and comply with this policy.

BACKGROUND TO THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

DEFINITIONS (DATA PROTECTION ACT 1998)

Personal Data	Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual.
Sensitive Data	Personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.
Data Controller	A person (or organisation) who determines the purposes for which and the manner in which any personal data is to be processed.
Data Subject	Any living individual who is the subject of personal data held by an organisation.
Processing	Obtaining, recording or holding the data or carrying out any operations on the data, including – organisation, adaptation or alteration of the data; retrieval, consultation or use of the data; disclosure of the data by transmission, dissemination or otherwise making available; alignment, combination, blocking, erasure or destruction of the information or data.
Third Party	Any individual/organisation other than the data subject or the data controller.
Relevant Filing System	A relevant filing system exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals. Personal data as defined and covered by the Act can be held in any format: electronic (including websites and emails), paper-based, photographic etc from which the individual's information can be readily extracted.

RESPONSIBILITIES UNDER THE DATA PROTECTION ACT

The school is the data controller under the Act. A Data Protection Officer is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the school. The Leadership Team and all those in managerial and supervisory roles are responsible for developing and encouraging good information handling practice within the school. Compliance with data protection legislation is the responsibility of all members of the school who process personal information. Members of the school are responsible for ensuring that any personal data supplied is accurate and up-to-date.

DATA PROTECTION PRINCIPLES

All processing of personal data must be done in accordance with the eight data protection principles.

1. *Personal data shall be processed fairly and lawfully.*

2. *Personal data shall be obtained for one or more specific and lawful purposes and not processed in a manner incompatible with those purposes.*

3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which it is held.*

4. *Personal data shall be accurate and, where necessary, kept up-to-date.*

5. *Personal data shall be kept only for as long as necessary.*

6. *Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.*

7. *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

8. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

SECURITY OF DATA

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. A judgement should be formed based upon the sensitivity and value of the information in question, but personal data should be kept:

in a lockable room with controlled access, or
in a locked drawer or filing cabinet, or
if computerised, password protected and/or encrypted or
kept on storage media which is secure, encrypted where relevant.

Care should be taken to ensure that computer screens are visible only to authorised staff and that computer passwords are kept confidential. Computers should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as 'confidential waste'. Hard drives of redundant computers should undergo secure electronic deletion before disposal.

This policy also applies to those who process personal data 'off-site'. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside the school.

DISCLOSURE OF DATA

The school must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter.

The Act permits certain disclosures without consent so long as the request is supported by appropriate paperwork.

RETENTION AND DISPOSAL OF DATA

The school discourages the retention of personal data for longer than it is required. Once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Students

In general, electronic student records containing information about individual students are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg shredding, disposal as confidential waste, secure electronic deletion).