Christ The King Sixth Form College
Data Protection Policy

Mission Statement

We are a Catholic College dedicated to the education and development of the whole person, so that all students can realise their full potential.

To achieve this as a community we will:

- Provide the highest standards of teaching and learning.
- Expect students to show commitment to their studies and the Christian values of the College.
- Provide equality of opportunity, with mutual respect and positive encouragement.
- Build and further develop a partnership with parents, schools, parishes, higher education, employers and the local community.
- Value staff and support their professional development.

In doing this we will reflect Christ's teaching in the life and work of the whole College.

1 Introduction

1.1 The Data Protection Act 1998 is intended to regulate the way information is collected and used. The College has developed its data protection policy in the context of the Act and its Catholic Mission.

1.2 We regard the lawful and correct treatment of personal information by the College as very important to the way we work and for maintaining confidence between ourselves and those with whom we deal. We therefore make every effort to ensure that personal information is treated lawfully and correctly.

1.3 We fully endorse and adhere to the principles of data protection, as detailed in the Data Protection Act 1998.

Specifically, the principles require that personal information:

(a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

(b) Shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.

(c) Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

(d) Shall be accurate and, where necessary, kept up to date.

(e) Shall not be kept for longer than is necessary for that purpose or those purposes.

(f) Shall be processed in accordance with the rights of data subjects under the Act.

(g) Shall not be transferred to a country or territory outside the European Economic area or Switzerland 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. The European Economic Area comprises of the following countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

and that:

(h) 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.

2 **Management of Data**

2.1 The Personnel Manager has overall responsibility for data protection in the College. The Personnel Manager is the data controller for information regarding employees and the Head of Student Services is the data controller for information regarding students.

2.2 Christ the King Sixth Form College will, through appropriate management, and application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information:
    - Meet its legal obligations to specify the purposes for which information is used.
    - Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Periodically review information that is held.
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken: the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as the wrong information.)
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.

2.3 In its capacity as employer the College needs to keep information about employees for purposes connected to their employment, including information on their recruitment, termination of their employment, training records, appraisal information and lesson observation notes. The sort of information held may include both computer and/or paper based records including information for payroll purposes, references, contact names and addresses and records relating to the employee's contract of employment.

2.4 These uses will be consistent with the employment relationship and with the principles of the Data Protection Act 1998. Such data may be processed only if it is necessary for the performance of an employee's contract with the College and/or is necessary for the purposes of exercising or performing any legal right or obligation of the College.

2.5 In its capacity as a provider of teaching and learning the College holds information about students which is both essential to support their progress and well being and also required by legislation. This includes data stored electronically and in paper format and comprises:

- Personal information including ethnicity and religion, and any notes made from private discussions with College Staff.
- Contact details of parents/guardians.
- Previous school, exam results attained and previous work experience and training.
- Details of any special requirements and/or learning needs.
- Performance monitoring details.
- Choice of course and course information including examination entry
- Attendance data.
- Copies of all correspondence.
- Copies of UCAS applications and information received on final destinations.
- Notes and minutes made from Counselling sessions.
- Copies of references sent and received by the College.

2.6 The College is legally obliged to disclose personal details held, to external authorities including the Police, Immigration Service, and Tax Inspectors in order to detect unlawful Activity. The College is required by law not to inform the student or member of staff. This includes information requested that relates to minors.

2.7 The College will inform parents of this legal obligation in relation to the Data Protection Act through correspondence issued during the start of the autumn term. Parents will be informed that, although rarely requested, if the appropriate authorities ask for information the College must disclose it without notifying parents.

3 Data Protection Principles

3.1 There are eight data protection principles which all staff in the College must comply with, although some staff will also have specific responsibilities, eg Personnel Manager and Head of Student Services. These principles are listed below and ensure that data is:

1 Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

2 Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

3 Adequate, relevant and not excessive for those purposes.

4 Accurate and kept up to date.

5 Not kept for longer than is necessary for that purpose.

6 Processed in accordance with the data subject's rights.

7 Kept safe from unauthorised access, accidental loss or destruction.

8 Not transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

3.2 In order to ensure the College complies with the Act the sections below replicate these numbered points. At Christ the King College:

3.2.1 All persons including staff, students, governors, contractors are entitled to:

- Know what categories of information the College holds and processes about them and why.
- Know how to request information.
- Know what the College is doing to comply with its obligations under the 1998 Act.

This information is available via the policy document site on the college Intranet. The College will obtain the consent of all staff and students regarding the holding and processing of data, unless the data has to be processed for legal purposes, eg Inland Revenue.

3.2.2 Holding of data which is adequate, relevant and not excessive.

Every two years the College will review the categories of data held on staff to ensure that it is still relevant.

The College will only hold data on students, which is required by legislation and is relevant and necessary to support their progress and well being. Each year the College is issued with a revised list of data requirements from its funding agency and other external agencies. An annual review is subsequently undertaken on all student documentation to ensure compliance.

3.2.3 The College will ensure that data is accurate and kept up to date.

The College will obtain information on staff through the application process and during their employment at Christ The King. The College will only hold data on staff, which it believes is entirely necessary for it to carry out its functions as an employer.

At enrolment, students are present when information is entered onto the main computer system and are asked to confirm accuracy. Each term, the College issues summary student and course information to students to confirm or correct

All staff are responsible for:

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date.

- Informing the College of any changes to information which they have provided, eg change of address.

- Checking the information that the College will send out from time to time.

- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College about them.

  Students are also responsible for informing the College of any changes to personal details, eg change of address, name.

3.2.4 Information will not be kept for longer than is necessary.

The College will hold information on staff for ten years from date of their resignation unless legal requirements or other issues to safeguard staff require the College to do otherwise eg pension data. Data will be disposed of safely by shredding or incineration, and will be kept securely until its destruction so that there is no accidental disclosure to third parties. Data from job applicants will be kept no longer than six months, except in the case of speculative applications where people request that details are kept on file.

Student records including personal information, academic achievements and conduct will be kept for ten years from the date that the student leaves.

Other records will be kept as follows:

Type of Record	**Suggested Retention Period**	**Reason for Length of Period**
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation.
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Disclosure and Barring Service (DBS) Criminal Record Checks (a) Certificate Unique Reference Number, Issue Date, Certificate Type (b) Certificate Contents	(a) 6 years from the end of employment (b) A maximum of six months, or longer in consultation with the DBS	(a) Safeguarding and Safer Recruitment and Selection Guidelines (b) Disclosure and Barring Service Code of Practice
Facts relating to redundancies where less than 20 redundancies	6 years from the date of redundancy	Time limits on litigation
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986

Type of Record	Suggested Retention Period	Reason for Length of Period
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health Records	6 years	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985
Student records, including academic achievements and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence	Limitation period for negligence.
	At least 10 years for personal and academic references.	Permits institution to provide references for a reasonable length of time.
	Certain personal data may be held in perpetuity.	While personal and academic references may become ‘stale’, some data e.g. transcripts of student marks may be required throughout the student’s future career. Upon the death of the data subject, data relating to him/her ceases to be personal data.

3.2.5 Personal data on staff, students and users will be processed in accordance with the rights described in the Act.

The College will always consider the rights of individuals in respect of their data. This means:

- Consent will be obtained if data is to be kept and used for any purpose.
- Individuals are entitled to know what data is kept about them and to whom it has been disclosed.
- No personal data will be disclosed to anyone outside or inside the College who does not strictly need to know that data for their job without the individual's consent.

Staff do not have the right to access certain information which is held about them. For example information held for management planning such as plans to promote, or make an employee redundant. Also staff cannot read references written by the College, although they are entitled to have access to this information when they have transferred to another organisation. This aspect of the policy has already been agreed and included in the Protocol for Drafting References (please see Policy Manual).

Sometimes it is necessary to process information which is sensitive for example about a person's health, criminal convictions. This may be to ensure that the College is a safe place for everyone or to operate College policies such as sick pay or equal opportunities. Because this information is sensitive and processing may cause anxiety to individuals, staff, students and users will be asked to give their express consent for this to take place.

Offers of employment or a place at the College may be withdrawn if an individual refuses to give consent without good reason.

Sensitive data will only be handled by designated staff unless the processing of data is in the best interests of the student or staff member.

Disclosure and Barring Service checks for new staff and students undergoing work experience will only be seen by those authorised to receive it in the course of their duties. A record is maintained of those to whom certificate information has been revealed and the College understands it is a criminal offence to pass this information to anyone who is not entitled to receive it.

The Data Protection Policy is consistent with policies in use in the College.

3.2.6 The College will ensure that all data relating to staff, students and users is held securely.

All staff are responsible for ensuring that:

- Any personal data which they hold is kept secure.
- Personal information is not disclosed either orally or in writing to any unauthorised third party unless transfers are made without consent, as expressed in the 1998 Act. For example, data may be disclosed to protect the vital interests of the data subject such as:
- The release of medical data where failure to release the data would result in harm to, or the death of, the data subject.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

All of the written information on staff, students and users will be held in offices and in non-portable locked desks or filing cabinets. Authorised administrators will monitor access to this information.

All of the information held electronically will only be accessible by authorised users. These users need to log-on to the system using a secure protocol.

Data stored electronically is backed up on a daily basis and a copy is stored in a separate secure location to ensure the prevention of accidental data loss

3.2.7 Information on staff, students and users will not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

4 Individual Rights Under the Data Protection Act

4.1 The College will ensure that individual rights under the Data Protection Act are safeguarded.

4.2 If an individual believes that the policy has been contravened he or she should raise the issue immediately:

- In the case of an employee this should be with the line manager or if the line manager is involved in the contravention, with the Personnel Manager.

- In the case of a student this should be with the relevant Head of Hall or if the Head of Hall is involved in the contravention, with the Head of Centre.

- In the case of other individuals this should be with the Personnel Manager.

If the issue cannot be resolved the individual has the right to make a complaint under the College complaints policy. The individual also has the right to request that the Information Commission make an assessment as to whether any provision in the Act has been contravened.

Reviewed: September 2015
Next Review Due: September 2017