

Data Protection Policy 2015

Castleknock Community College



Review Dates

Staff	January 2015	Reviewed
Parents	January 2015	Reviewed
Student Council	February 2015	Reviewed
BOM	March 2015	Ratified

Due for next review March 2017

Contents

1. Introductory Statement	Page 2
2. Data Protection Principles	Page 3
3. Scope	
4. Definition of Data Protection Terms	Page 4
5. Rationale	
6. Other Legal Obligations	Page 5
7. Relationship to characteristic spirit of the College's mission statement and educational aims	Page 6
8. Personal Data	Page 5
8.1 Staff Records	
8.2 Student Records	
8.3 Board of Management records	
8.4 Other Records	
8.4.1. Creditors	
8.4.2. CCTV images/recording	
8.4.3 Examination results	
8.4.4. October Returns	
9. Links to other policies and to curriculum delivery	Page 11
10. Processing in line with data subject's rights	Page 12
11 Dealing with a data access requests	Page 12
12 Providing information over the phone	Page 13
13. Implementation arrangements, roles & responsibilities	Page 13
14. Ratification & communication	Page 13
15. Monitoring the implementation of the policy	Page 14
16. Reviewing & evaluating the policy	Page 14

The Mission Statement of Castleknock Community College

We the pupils, parents and staff of Castleknock Community College, strive for excellence in a caring and supportive environment. Growing and developing through co-operation will enable all to realise their full potential.

1. Introductory Statement

The College's Data Protection Policy applies to the personal data held by the College which is protected by the Data Protection Acts 1988 and 2003.

The policy applies to all College staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the College) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the College.

2. Data Protection Principles

The College is a data controller of personal data relating to its past, present and future staff, students, parents/guardians and other members of the College community. As such, the College is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

Obtain and process Personal Data fairly: Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous Schools/Colleges. In relation to information the College holds on other individuals (members of staff, individuals applying for positions within the College, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the College. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

Keep it only for one or more specified and explicit lawful purposes: The College will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

Process it only in ways compatible with the purposes for which it was given initially: Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

Keep Personal Data safe and secure: Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in

the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the College premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

Keep Personal Data accurate, complete and up-to-date: Students, parents/guardians, and/or staff should inform the College of any change which the College should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the College will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

Ensure that it is adequate, relevant and not excessive: Only the necessary amount of information required to provide an adequate service will be gathered and stored.

Retain it no longer than is necessary for the specified purpose or purposes for which it was given: As a general rule, the information will be kept for the duration of the individual's time in the College. Thereafter, the College will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the College will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The College may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

Provide a copy of their personal data to any individual, on request: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

3. Scope

Purpose of the Policy: The Data Protection Acts 1988 and 2003 apply to the keeping and processing of Personal Data, both in manual and electronic form. The purpose of this policy is to assist the College to meet its statutory obligations, to explain those obligations to College staff, and to inform staff, students and their parents/guardians how their data will be treated.

The policy applies to all College staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the College) insofar as the College handles or processes their Personal Data in the course of their dealings with the College.

4. Definition of Data Protection Terms

In order to properly understand the College's obligations, there are some key terms which should be understood by all relevant College staff:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it forms part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller i.e. the College.

Sensitive Personal Data refers to Personal Data regarding a person's:

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the Board of Management while the Principal will implement the policy on behalf of the Board.

5. Rationale

In addition to its legal obligations under the broad remit of educational legislation, the College has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003. This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the College's legal responsibilities has increased.

The College takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the principal and board of management to make decisions in respect of the efficient running of the College. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the College and board of management.

6. Other Legal Obligations

Implementation of this policy takes into account the College's other legal obligations and responsibilities. Some of these are directly relevant to data protection. *For example:*

- ***Under Section 9(g) of the Education Act, 1998***, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the College relating to the progress of the student in their education
- ***Under Section 20 of the Education (Welfare) Act, 2000***, the College must maintain a register of all students attending the College
- ***Under section 20(5) of the Education (Welfare) Act, 2000***, a principal is obliged to notify certain information relating to the child's attendance in College and other matters relating to the child's educational progress to the principal of another College to which a student is transferring
- ***Under Section 21 of the Education (Welfare) Act, 2000***, the College must record the attendance or non-attendance of students registered at the College on each College day
- ***Under Section 28 of the Education (Welfare) Act, 2000***, the College may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other Colleges, other centres of education) provided the College is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)
- ***Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004***, the College is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOS")) such information as the Council may from time to time reasonably request
- ***The Freedom of Information Act 1997*** provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While Colleges are not currently subject to freedom of information legislation, if a College has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body
- ***Under Section 26(4) of the Health Act, 1947*** a College shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the College) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection

- **Under *Children First: National Guidance for the Protection and Welfare of Children* (2011)** published by the Department of Children & Youth Affairs, Colleges, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

7. Relationship to characteristic spirit of the College's mission statement & educational aims

Castleknock Community College seeks to

- enable each student to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The College wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

8. Personal Data

The *Personal Data* records held by the College **may** include:

8.1. Staff records:

Categories of staff data: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the College, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on College property or in connection with the staff member carrying out their College duties
- Records of any reports the College (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

Purposes: Staff records are kept for the purposes of:

- the management and administration of College business (now and in the future)
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.

- to enable the College to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- to enable the College to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- and for compliance with legislation relevant to the College.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: These records are securely held in a digital format and all manual records and correspondence is securely held in the relevant filing system.

8.2. Student records:

Categories of student data: These may include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the College. These records may include:
 - Name, address and contact details, PPS number
 - Date and place of birth
 - Names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
 - Religious belief
 - Racial or ethnic origin
 - Membership of the Traveller community, where relevant
 - Whether they (or their parents) are medical card holders
 - Whether English is the student's first language and/or whether the student requires English language support
 - Any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
 - Information on previous academic record (including reports, references, assessments and other records from any previous College(s) attended by the student
 - Psychological, psychiatric and/or medical assessments
 - Attendance records
 - Photographs and recorded images of students including at College events and noting achievements. At the time of enrolment all parent(s)/guardian(s) are required to sign consent forms regarding the *"Taking and Using Images of Children in Colleges"*
 - Academic record – subjects studied, class assignments, examination results as recorded on official College reports
 - Records of significant achievements
 - Whether the student is repeating the Leaving Certificate
 - Whether the student is exempt from studying Irish
 - Records of disciplinary issues/investigations and/or sanctions imposed

- Garda vetting outcome record (where the student is engaged in work experience organised with or through the College/DDL ETB which requires that they be Garda vetted).
- Other records e.g. records of any serious injuries/accidents etc.
- Records of any reports the College/DDL ETB have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

Purposes: The purposes for keeping student records are:

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of College closure or to inform parents of their child's educational progress or to inform parents of College events etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate College achievements, compile yearbooks, establish a College website, record College events, and to keep a record of the history of the College. Such records are taken and used in accordance with the College's "Guidance for Taking and Using Images of Pupils in Colleges"
- to ensure that the student meets the College's admission criteria
- to ensure that students meet the minimum age requirements for their course,
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Colleges etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the College will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: These records are securely held in a digital format and all manual records and correspondence is securely held in the relevant filing system.

8.3. Board of management records:

Categories of board of management data: These may include:

- Name, address and contact details of each member of the Board of Management (including former members of the Board of Management).
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.

Purposes: To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

Location: In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access.

Security: These records are securely held in a digital format and all manual records and correspondence is securely held in the relevant filing system.

8.4. Other records:

The College will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database).

8.4.1. Creditors

Categories of data: the College may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- name
- address
- contact details
- PPS number
- tax details
- bank details and
- amount paid.

Purposes: This information is required for routine management and administration of the College's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: These records are securely held in a digital format and all manual records and correspondence is securely held in the relevant filing system.

8.4.2. CCTV images/recordings

Categories: CCTV are installed in the College, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.

Purposes: Safety and security of staff, students and visitors and to safeguard College property and equipment.

Location: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in a secure area adjacent to the deputy principal's office.

Security: Access to images/recordings is restricted to the principal, deputy principals and one assistant principal. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

8.4.3. Examination results

Categories: The College will hold data comprising examination results in respect of its students. These include class, house, annual, continuous assessment and mock- examinations results.

Purposes: The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: These records are securely held in a digital format and all manual records and correspondence is securely held in the relevant filing system.

8.4.4. October Returns

Categories: At the beginning of each academic year (and for 1st year or transferring students, on enrolment) parents/guardians and students are asked to provide the College with certain information so that the College can make returns to the Department of Education and Skills ("DES") referred to as "October Returns". These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The October Return contains individualised data (such as an individual student's PPS number) which acts as an "identifier" for the DES to validate the data that belongs to a recognised student.

The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection

pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes.

The DES has a data protection policy which can be viewed on its website (www.education.ie).

The DES has also published a “Fair Processing Notice” to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the “Circulars” section).

Purposes: The College asks parents/guardians and students to forward information which will form part of the October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the College.

The main purpose of the October Returns is for the DES to determine whether the student qualifies for English language support and/or additional resources and support to meet their particular educational needs.

The October Returns are submitted to the DES electronically. The DES has their own policy governing the security of the data sent to them by all post-primary Colleges. The co-operation of each student and/or their parents/guardians in completing the October Return is greatly appreciated as the College’s aim is to ensure that each student is assisted in every way to ensure that s/he meets his/her full potential.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: These records are securely held in a digital format and all manual records and correspondence is securely held in the relevant filing system.

9. Links to other policies and to curriculum delivery

Our College policies need to be consistent with one another, within the framework of the overall College Plan. Relevant College policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy
- Counter-Bullying Policy
- Code of Behaviour
- Admissions/Enrolment Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/RSE Policy.

10. Processing in line with data subject's rights

Data in this College will be processed in line with the data subjects' rights.

Data subjects have a right to:

- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended (e.g. family details, exam results, attendance etc.)
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. Dealing with a data access requests

Section 3 access request

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the College holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request

Individuals are entitled to a copy of their personal data on written request.

The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)

- Request must be responded to within 40 days
- Fee may apply but cannot exceed €6.35
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the College as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the College refuse to furnish the data to the applicant.

12. Providing information over the phone

In our College, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the College over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

13. Implementation arrangements, roles and responsibilities

In our College the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

14. Ratification & communication

When the Data Protection Policy has been ratified by the board of management, it becomes the College's agreed Data Protection Policy. It should then be dated and circulated within the College community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the College community.

Parents/guardians and students will be informed of the Data Protection Policy from the time of enrolment of the student by including a summary the Data Protection Policy as part of the Enrolment Process.

15. Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the principal and a sub-committee of the board of management.

At least one annual report should be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

16. Reviewing and evaluating the policy

The policy should be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), legislation and feedback from parents/guardians, students, College staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of College planning.

