Crescent College Comprehensive SJ

DATA PROTECTION POLICY

11 October 2017

A.M.D.G.

CRESCENT COLLEGE COMPREHENSIVE S.J.

Data Protection Policy

Introductory Statement

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

The policy applies to all school 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 school) 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 school.

Data Protection Principles

The school is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school 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. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, 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 School. 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 School 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 school 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 school of any change which the school 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 school 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 school. Thereafter, the school 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 school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school 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.

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 school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

The policy applies to all school 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 school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

In order to properly understand the school's obligations, there are some key terms which should be understood by all relevant school 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 form 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 school.

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 of Crescent College Comprehensive SJ.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school 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 school's legal responsibilities has increased.

The school 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 School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

Other Legal Obligations

Implementation of this policy takes into account the school'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 school relating to the progress of the student in their education

- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School

- 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 school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring

- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day

- Under Section 28 of the Education (Welfare) Act, 2000, the School 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 schools, other centres of education) provided the School 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 school 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 schools are not currently subject to freedom of information legislation, if a school 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 School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) 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, schools, 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).

Relationship to characteristic spirit of the School (School's mission/vision/aims)

Crescent College Comprehensive SJ seeks to:

incorporate the Characteristics of Jesuit Education. It seeks to develop fully each student's religious, moral, social, intellectual, physical and cultural sensibilities. As an important means of doing this the school strives to create a strong sense of community between parents, students and teachers.

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 school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

Personal Data

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

A. Staff records:

(a) **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 school, 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 school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (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).

(b) **Purposes**: Staff records are kept for the purposes of:

- the management and administration of school business (now and in the future)
- to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- to facilitate pension payments in the future
- human resources management
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school 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 school 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 school.

(c) **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.

(d) **Security:** Records are stored both in paper format and digitally. Digitally stored data is accessed to relevant school personnel only by password. Files that are in paper form with data are stored in the Accountant's office in a locked filing cabinet.

Student records:

(a) **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 school. It is the responsibility of parents/guardians to inform the school of any update to their child's data. 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 school(s) attended by the student
- psychological, psychiatric and/or medical assessments
- attendance records
- academic record – subjects studied, class assignments, examination results as recorded on official School 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 school which requires that they be Garda vetted)
- other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- records of any reports the school (or its employees) 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).

(b) **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 school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's "Guidance for Taking and Using Images of Pupils in Schools"
- to ensure that the student meets the school'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 Schools 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 School 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.

(c) **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.

(d) **Security:** Student records are stored both electronically and in manual file format. Only relevant personnel in the school may have access to such records e,g. Principal, Deputy Principal, Year Head, access on computer record for relevant personnel is coded and pass worded. Any data of a sensitive nature is kept on manual file in a key locked filing cabinet in the principal's office accessed only by the principal or with the principal's consent if any relevant person needs appropriate access. Past Pupil/ student records are held in a locked Archive Room.

C. ***Board of Management records:***

(a) **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)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.

(b) **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.

(c) **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.

(d) **Security:** Manual files stored in locked filing cabinet in Principal's office. Student Support Worker and School Secretary has copy of contact details of Board of Management for the purpose of sending correspondence etc.

D. ***Other records:***

Records of a sensitive nature e.g. complaints, Child protection issues, etc. are kept manually in locked filing cabinet in Principal's office and in locked safe in Administration office.

Creditors

(a) **Categories of data**: the school 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.

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

(c) **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.

(d) **Security:** Records are stored both in paper format and digitally. Digitally stored data is accessed to relevant school personnel only by password. Files that are in paper form with data are stored in the Accountant's office in a locked filing cabinet.

Charity tax-back forms

(a) **Categories of data**: the school may hold the following data in relation to donors who have made charitable donations to the school:
   a. name
   b. address
   c. telephone number
   d. PPS number
   e. tax rate
   f. signature and
   g. the gross amount of the donation.

(b) **Purposes**: Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.

(c) **Location**: In a secure, locked filing cabinet in the Accountant's Office, that only authorised school personnel (e.g. Accountant, can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** Records are stored both in paper format and digitally. Digitally stored data is accessed to relevant school personnel only by password. Files that are in paper form with data are stored in the Accountant's office in a locked filing cabinet.

CCTV images/recordings

(a) **Categories**: CCTV is installed in Crescent College Comprehensive SJ 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.

(b) **Purposes**: Safety and security of staff, students and visitors and to safeguard school property and equipment.

(c) **Location**: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in a locked cabinet in the ICT Office.

(d) **Security:** Access to images/recordings is restricted to school authorised personnel e.g. the principal & deputy principal of the school. 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.

Examination Results

(a) **Categories**: The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock- examinations results.

(b) **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.

(c) **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.

(d) **Security:** locked filing cabinet in administration office of the school that only authorised school personnel (e.g. Principal, DP and/or clerical officers) can access. In house examination results are held electronically where relevant persons have access through personalised passwords.

October Returns

(a) **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 school with certain information so that the School 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).

(b) **Purposes:** The school asks parents/guardians and students to complete October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school. 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 schools. The co-operation of each student and/or their parents/guardians in completing the October Return is greatly appreciated as the school's aim is to ensure that each student is assisted in every way to ensure that s/he meets his/her full potential.

(c) **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.

(d) **Security:** The school uses P-Pod which is the DES data database package which only relevant personnel have any access i.e. school secretary, Deputy principal and Principal. The school's Administration package is CMIS Facility. Staff access relevant data through pass worded laptops/computers and CMIS Facility requires unique teacher passwords, which are not automatically saved.

Links to other policies and to curriculum delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school 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
- Anti-Bullying Policy
- Code of Behaviour
- Admissions/Enrolment Policy
- CCTV Policy
- SPHE/CSPE etc.

Processing in line with data subject's rights

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

Data subjects have a right to:

(a) Request access to any data held about them by a data controller
(b) Prevent the processing of their data for direct-marketing purposes
(c) Ask to have inaccurate data amended
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

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 school 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 school 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 school refuse to furnish the data to the applicant.

Providing information over the phone

In our school, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school 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.

Implementation arrangements, roles and responsibilities

In our school 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

Ratification & communication

When the Data Protection Policy has been ratified by the board of management, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the school 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 school community.

Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Enrolment Pack, by either enclosing it or incorporating it as an appendix to the enrolment form.

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.

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 should 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, school staff and others. The policy should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

This policy was ratified by the Board of Management of Crescent College Comprehensive SJ

On Date: 11th October 2017

Helen O'Donnell

Helen O'Donnell, Chairperson
Board of Management

Karin Fleming

Karin Fleming, Secretary
Board of Management

Appendix 1

A.M.D.G.
CRESCENT COLLEGE COMPREHENSIVE S.J.

Data Access Request Form

Request for a copy of Personal Data under the Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Date issued to data subject:

Important: Proof of Identity must accompany this Access Request Form if it is a Seciton 4 Data Access Request together with proof of identity documents such as driver's licence, passport).

A fee of €6.35 must accompany this Access Request Form if it is a Section 4 Data Access Request together with proof of identity (eg, official/State photographic identity document such as a driver's licence, passport).

Full Name	
Maiden Name *(if name used during* your school duration*)*	
Address	
Contact number *	Email addresses *

** We may need to contact you to discuss your access request*

Please tick the box which applies to you:

Student ☐	Parent/Guardian of student ☐	Former Student ☐	Current Staff ☐	Former Staff ☐
Age: Year group/class:	Name of Student:	Insert Year of leaving:		Insert Years From/To:

Section 3 Data Access Request:

I, _____ (insert name) wish to be informed whether or not Crescent College Comprehensive SJ holds personal data about me/my child and to be provided with a description of this data and to be informed of the purpose for such data. I am making this access request under **Section 3** of the Data Protection Acts.

OR

Section 4 Data Access Request:

I, _____ (insert name) wish to make an access request for a copy of any personal data that Crescent College Comprehensive SJ holds about me/my child. I am making this access request under Section 4 of the Data Protection Acts.

Section 4 Data Access Request only: I attach €6.35

Any other information relevant to your access request (eg., if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings (otherwise it may be very difficult or impossible for the school to locate the data).

Signed: _____ **Date: _____**

Checklist – Have you:

1.	*Completed the Access Request Form in full?*	____
2.	*Included a cheque or postal order made payable to Crescent College Comprehensive SJ in the amount of €6.35 where Section 4 request is made? (Please do not send €6.35 if you are making a request under Section 3. There is no administration charge for a Section 3 request, and if you send us a cheque, it will be returned to you).*	____
3.	*Signed and dated the Access Request Form?*	____
4.	*Included a photocopy of official/State photographic Identity document (driver's licence, passport, etc.)*	____

Note: The school should satisfy itself as to the identity of the individual and make a note in the school records that identity has been provided, but the school should not retain a copy of the identity document.

Please return this form to: The Principal, Crescent College Comprehensive SJ, Dooradoyle, Limerick

Appendix 2

Records Retention Schedule
Crescent College Comprehensive SJ

Retention of Records

Crescent College Comprehensive SJ in its role as a Data Controller, is conscious of its statutory obligations to be fully transparent in relation to the length and time for which personal data will be kept. The Board of Management has put in place procedures to ensure compliance with all directives in relation to the storing and retention of data sought by the school.

Attached are listed guidelines to the length of time various categories of data are stored at the school.

Appendix 3

Exceptions to the Right of Access

Individuals have a strong right of access to see their personal data. However, section 5 of the Data Protection Acts provides that individuals do not have a right to see information relating to them where any of the following circumstances apply.

If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities
Comment: It would obviously be unacceptable to allow a criminal suspect to see all of the information kept about him by An Garda Síochána, where this would be likely to impede the effectiveness of the criminal investigation. On the other hand, however, if allowing an individual access to personal information about him or her would not be likely to impede an investigation, then the access request would have to be complied with. (see case study 2/04)
If granting the right of access would be likely to impair the security or the maintenance of good order in a prison or other place of detention

If the information is kept for certain anti-fraud functions: but only in cases where allowing the right of access would be likely to impede any such functions

If granting the right of access would be likely to harm the international relations of the State

If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation

If the information would be subject to legal professional privilege in court

If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved

If the information is back-up data.
Comment: It would be unreasonable to expect an organisation to retrieve back-up copies of its personal information in responding to an access request. However, it should be noted that back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual's right of access in the normal way.