

# **Blackrock College**



## **Data Protection Policy**

## Summary of Policy Changes

### Revision History

Date of creation: 10 May 2018

Date of this revision: 28 May 2019

Date of next revision: 28 May 2020

Version Number/ Revision Number	Revision Date	Summary of Changes
1.0	10 May 2018	Policy created and approved by the Board of Management
2.0	30 July 2019	Updated and revised:  Explanation of Data Subject Rights expanded  The following Appendices added:  Glossary, Personal Data and Related Processing purposes, Categories of recipients, implementing the data processing principles, managing rights requests, reference cites



# Blackrock College

## Data Protection Policy

May 2018

The characteristic spirit of Blackrock College (the College) has at its core a desire to promote and protect the dignity of every member of its community: students, staff and parents. This includes respect for the protection of data stored at the school and for the right of access to this data. This policy is informed by the General Data Protection Regulation (EU) 2016/679. The policy applies to all school staff, the Board of Management, parents/guardians, students, (including prospective students) their parents/guardians, applicants for positions within the school and service providers with access to school data. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

### Data Protection Principles

The Board of Management 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 the General Data Protection Regulation (EU) 2016/679 which can be summarised as follows:

- **Obtain and process *Personal Data* fairly, lawfully and in a transparent manner:** 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 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 and/or compiled during the course of employment as a part of the contractual agreement on the understanding that the school requires such information to carry out its legitimate role as an employer and as a provider of education services to the pupils seeking to be enrolled and once they are enrolled. All such data is treated in accordance with the GDPR 2016/679 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.

## Scope

**Purpose of the Policy:** The General Data Protection Regulation (EU) 2016/679 applies 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 school handles or processes their *Personal Data* in the course of their dealings with the school.

## Safeguarding Against Data Protection and Security Risks

This policy helps to protect Blackrock College from data security risks, including:

- Breaches of security and confidentiality. For instance, information being given out inappropriately.
- Reputational damage. For instance, the College could suffer if hackers successfully gained access to sensitive data.
- The risk of large fines or sanctions being imposed by the authorities.

## 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 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, Blackrock College.

### Rationale

In addition to its legal obligations under the broad remit of educational legislation, the College has a legal responsibility to comply with the General Data Protection Regulation (EU) 2016/679.

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 the Board of Management.

### 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 the College 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 College must record the attendance or non-attendance of students registered at the College on each school 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 schools, 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 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* (2017) 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) and/or An Garda Síochána in the event of knowledge or belief of a serious crime having been committed against a child or vulnerable person.

### Relationship to Characteristic Spirit of the College (Spiritan Ethos)

Blackrock 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.

### Personal Data

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

#### 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 school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number
- Contract of employment and any amendments to it
- Original records of application and appointment to promotion posts
- Financial information records
- Payroll records
- Employee review meetings
- Grievance and disciplinary procedures information
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Information relating to your health, which could include reasons for absence and GP reports and notes
- 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 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)
- CCTV Footage (Please see Blackrock College CCTV Policy for more details)



**Purposes:** Staff records are kept for the purposes of:

- the management and administration of College 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 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.

**Lawful basis for processing:** Legal obligation for certain types of information such as deduction of income tax.

For the performance of a contract.

Article 9(2b) GDPR states that special categories of data (eg. Health data) can be processed when: *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment.*

To protect a member of staff's vital interest.

Because it is in the public interest or in the exercise of the official authority vested in the College.

**Location:** Staff records are kept in the following locations of Blackrock College: Head of Finance, HR Office, Principal Secretary's Office and Deputy Principal's Office. Manual Records are held in relevant filing system, in a secure, locked filing cabinet that only personnel who are authorised to use the data can access on a 'need-to-know' basis. Soft copies of staff records are also kept on "Europay" payroll software and Accounts softwares such as "Access" and "Ardbrook". Employees are required to maintain the confidentiality of any data to which they have access.

**Security:** Manual records are kept in a secure filing cabinet in locked offices. An automated access control system is in place and the Department of Finance is protected by installed alarm system. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** Relevant data is passed onto the relevant government agencies for tax and social security reasons. Relevant data is passed onto the school's pension and life assurance providers for the purposes of those schemes. The following list includes examples of such organisations but is not exhaustive: Department of Education and Skills, Insurance Company, Health and Safety Authority, Workplace Relations Commission, Revenue Commissioners.

*Note: Data Collected Through Garda Vetting*

*Blackrock College understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns, the information will be dealt with on a confidential basis. All information pertaining to such a situation will be stored in the same way as other data. The Board of Management will not pass on a copy of a Garda Vetting Form to any other party.*



**Retention period:** Please see Appendix 1 - Records Retention Schedule.

**Students' 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 school(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).
- Video of school events including recordings of rugby matches for educational purposes and internal use only
- 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 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 College (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)
- Images/photo (including CCTV) (Please see Blackrock College CCTV Policy for more details)

**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 spiritual, educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate College achievements, compile College annuals, 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 Schools"
- 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 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 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 for future reference requests
- pastoral purposes

**Please see Appendix 3 for further details regarding Students' Personal Data and Related Processing Purposes.**

**Lawful basis for processing:**

- Legal basis for some information (as noted above).
- For the performance of a contract for certain types of information.
- Consent for all categories of sensitive information (as listed above)
- To protect a pupil's vital interest.
- Because it is in the public interest or in the exercise of the official authority vested in the school

**Location:** Student manual records are kept in the following locations of Blackrock College: Principal's Office, Principal Secretary's Office, Deputy Principals' Offices, Deans' Offices and Hall of Residence Department (Boarding School). All manual Records are held in relevant filing system, in a secure, locked filing cabinet that only personnel who are authorised to use the data can access on a 'need-to-know' basis. Soft copies of student records are also stored in the following GDPR compliant electronic locations: Moodle (open-source learning platform), Student Information Management System (SIMS), EduLink One (integrated school information platform), REACH (School Boarding House Software) and P-POD (Post Primary Online Database). Students' names and parents' e-mail addresses are also held on Counter Solutions (cashless cloud platform) individual accounts.

Employees are required to maintain the confidentiality of any data to which they have access.

**Security:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** From time to time it may be necessary for us to transfer student's personal data on a private basis to other bodies (including the Department of Education & Skills, Educational Research Centre (ERC), State Examinations Commission, the Department of Social Protection, An Garda Síochána, the Health Service Executive, Tusla, social workers or medical practitioners, the National Educational Welfare Board, the National Council for Special Education, any Special Education Needs Organiser, the National Educational Psychological Service, or (where the student is transferring) to another school. Only relevant data is passed onto the relevant state agencies as noted under the legal basis for collecting information.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including GDPR compliant IT providers, security providers,



legal advisors etc). We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

**Please see Appendix 4 for further information regarding Categories of Recipients that personal data may be shared with.**

**Retention period:** Students' personal data is retained for 25 years for references and pastoral purposes. A detailed outline of how long it is retained is available in Appendix 1 of the Data Protection Policy on our website.

#### **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)
- 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
- Garda Vetting Forms

**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.

**Lawful basis for processing:** Legal basis

**Location:** Board of Management records are kept in Principal Secretary's office of Blackrock College. Manual Records are held in relevant filing system, in a secure, locked filing cabinet that only personnel who are authorised to use the data can access on a 'need-to-know' basis. Employees are required to maintain the confidentiality of any data to which they have access

**Security:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** Relevant data on the Finance Sub-Committee of the Board of Management minutes is passed onto the College Auditors.

**Retention period:** Please see Appendix 1 - Records Retention Schedule.

#### **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). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

#### **Parents' Records:**

**Categories of data:** Blackrock College may hold some or all of the following information about parents and/or guardians of pupils: Names and addresses of parents/legal guardians and their contact details (including any special arrangements with regard to guardianship, custody or access) and place of work; religious belief; financial information and fees related correspondence.



**Purposes:**

- 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 enable the College to manage financial affairs, including the issuing of fee invoices
- The performance of the contract
- To manage our business for our legitimate interest
- To maintain appropriate control of finances and to plan the College's future
- For collection of fees and charges
- Credit management including collecting and enforcing debts and arrears
- To inform all parents of developmental activities on campus
- Future reference requests and pastoral purposes
- Communication purposes

**Lawful basis for processing:** For the performance of a contract for certain types of information.

**Location:**

Parents' records are kept in the following locations of Blackrock College: Principal's Office, Secretary's Office, Deputy Principals' Offices, Hall of Residence Department (Boarding School) and Department of Finance. All manual Records are held in relevant filing system, in a secure, locked filing cabinet that only personnel who are authorised to use the data can access on a 'need-to-know' basis. Soft copies of parents' records are also stored in the following GDPR compliant electronic location: Student Information Management System (SIMS), REACH (School Boarding House Software). Students' names and parents' e-mail addresses are also held on Counter Solutions (cashless cloud platform) individual accounts.

Employees are required to maintain the confidentiality of any data to which they have access.

**Security:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:**

To abide by Blackrock College and Willow Park Schools Fees Policy (Campus Fees Policy which is available on our web site) and for the purposes noted above we may share your data with the following bodies:

- Willow Park Junior School Finance Sub-Committee of the Board of Management, Willow Park Senior School Finance Sub-Committee of the Board of Management to review instances of overdue balances and decide on the appropriate course of action
- Relevant data may be passed onto the College's solicitor or for third party debt collection in the event of outstanding fees, and may be passed to our Auditors where relevant in the performance of their duties
- Blackrock College Development Office through Student Information Management System (SIMS)
- GDPR compliant SendMode bulk messaging service for the purposes stated above. Your phone number will be shared with SendMode service provider
- Parents' Association – Year Committee Chair and Communication Representatives

**Retention period:**

- As a general rule financial information data is kept for 7 years, unless there are outstanding fees due or another family member is still a pupil on campus. All the information will be disposed 7 years after the last member of the family leaves the campus or the outstanding balance is discharged
- Other parents' personal data is kept for 25 years for future reference requests and pastoral purposes



### **Creditors/Debtors**

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

- name
- address
- contact details
- PPS number
- tax details
- bank details, and
- amount paid/due
- invoices and/or charges, and
- debtors financial circumstances and notes of communications

**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.

**Lawful basis for processing:** Legal basis

**Location:** In a secure, locked filing cabinet in the Department of Finance 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:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** Relevant data is passed onto the Revenue Commissioners and may be passed to College Auditors where relevant in the performance of the duties.

**Retention period:** As a general rule this type of data is kept for 7 years and then it is confidentially disposed.

### **Charity Tax-back forms**

**Categories of data:** the school may hold the following data in relation to donors who have made charitable donations to the school:

- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

**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 College to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate



certificate is the parent's name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the College in the case of audit by the Revenue Commissioners.

**Lawful basis for processing:** Legal basis

**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:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** Relevant data is passed onto the Revenue Commissioners.

**Retention period:** As a general rule this type of data is kept for 7 years and then it is confidentially disposed.

### **CCTV images/recordings**

**Categories:** Closed Circuit Television Systems (CCTVS) are installed in Blackrock College. CCTV systems are installed (both internally and externally) in the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. These CCTV systems may record images of staff, students and members of the public who visit the premises. A detailed description of CCTV system and its purposes is outlined in Blackrock College CCTV Policy.

**Purposes:** CCTV surveillance at Blackrock College is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours;
- promoting the health and safety of staff, pupils and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Gardai in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the school rules are respected so that the school can be properly managed.

**Lawful basis for processing:** Legitimate interests.

**Location:** Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in a secure locked cabinet on the premises. The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Blackrock College has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.

**Security:** Access to images/recordings is restricted to the Principal, Deputy Principals, Deans, Management PCs and reception of Blackrock College. 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 the General Data Protection Regulation (EU) 2016/679.



**Sharing data:** CCTV images/recordings may be passed to An Garda Síochána and any other relevant state agency or body.

**Retention period:** Please see Appendix 1 - Records Retention Schedule.

### **Examination Results**

**Categories:** The College will hold data comprising examination results in respect of its students. These include class, mid-term, 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.

**Lawful basis for processing:** legal basis

**Location:** Examination results are kept in Principal's Secretary Office. Manual Records are held in relevant filing system, in a secure, locked filing cabinet that only personnel who are authorised to use the data can access on a 'need-to-know' basis. Soft copies of student records are also stored on open-source learning platform Moodle, Student Information Management System (SIMS) and EduLink One (integrated school information platform). Employees are required to maintain the confidentiality of any data to which they have access.

**Security:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** Examination results are not shared with any external body.

**Retention period:** Please see Appendix 1 - Records Retention Schedule.

### **October Returns**

**Categories:** At the beginning of each academic year (and for 2nd 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](http://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](http://www.education.ie) (search for Circular Letter 0047/2010 in the "Circulars" section).

**Purposes:** The College 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 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 its 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 College's aim is to ensure that each student is assisted in every way to ensure that he meets his full potential.

#### **Lawful basis for processing: legal basis**

**Location:** October returns are kept in Principal's Office. Manual Records are held in relevant filing system, in a secure, locked filing cabinet that only personnel who are authorised to use the data can access on a 'need-to-know' basis. Employees are required to maintain the confidentiality of any data to which they have access.

**Security:** Manual records are kept in a secure filing cabinet in locked offices. Computer records are kept on password protected PCs by up to date security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties. Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractor. Computer systems access the internet only through an approved internet firewall or other security device. Firewall and anti-virus software are regularly updated and routinely renewed before licences expire. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the information.

Our computer-held data has an off-site back-up procedure to monitor our daily backups and ensure that they are performed in line with best practice.

Information on computer screens and manual files are kept hidden from callers to the school offices.

All waste papers, printouts are disposed of in a secure manner. Only authorised people are able to access, alter, disclose or destroy personal data.

There is an automatic door and control system in place in Blackrock College.

Blackrock College will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Blackrock College acknowledges that high standards of security are essential for processing all personal information.

**Sharing data:** Relevant data is passed onto the Department of Education

**Retention period:** Please see Appendix 1 - Records Retention Schedule.

### **Data Subject's Rights**

- 1.1 **Your Rights** Personal Data will be processed by the school in a manner that is respectful of the rights of data subjects. Under GDPR these include<sup>1</sup>
  - (i) the right to information
  - (ii) the right of access
  - (iii) the right to rectification
  - (iv) the right to erasure ("right to be forgotten")
  - (v) the right to restrict processing
  - (vi) the right to data portability
  - (vii) the right to object
  - (viii) the right not to be subject to automated decision making
  - (ix) the right to withdraw consent
  - (x) the right to complain.
- 1.2 **Right to be Informed** You are entitled to information about how your personal data will be processed. We address this right primarily through the publication of this Data Protection Policy. We also publish additional privacy notices/statements which we provide at specific data collection times, for example, our Website Data Privacy Statement is available to all users of our website. Should you seek further

<sup>1</sup> For further information on your rights see [www.GDPRandYOU.ie](http://www.GDPRandYOU.ie).



clarification, or information that is not explicit in our Policy or Privacy Statements, then you are requested to forward your query to the school.

- 1.3 **Right of Access** You are entitled to see any information we hold about you. The school will, on receipt of a request from a data subject, confirm whether or not their personal data is being processed. In addition, a data subject can request a copy of their personal data. The school in responding to a right of access must ensure that it does not adversely affect the rights of others.
- 1.4 **Right to rectification** If you believe that the school holds inaccurate information about you, you can request that we correct that information. The personal record may be supplemented with additional material where it is adjudged to be incomplete.
- 1.5 **Right to be forgotten** Data subjects can ask the school to erase their personal data. The school will act on such a request providing that there is no compelling purpose or legal basis necessitating retention of the personal data concerned.
- 1.6 **Right to restrict processing** Data subjects have the right to seek a restriction on the processing of their data. This restriction (in effect requiring the controller to place a "hold" on processing) gives an individual an alternative to seeking erasure of their data. It may also be applicable in other circumstances such as where, for example, the accuracy of data is being contested.
- 1.7 **Right to data portability** This right facilitates the transfer of personal data directly from one controller to another. It can only be invoked in specific circumstances, for example, when processing is automated and based on consent or contract.
- 1.8 **Right to object** Data subjects have the right to object when processing is based on the school's legitimate interests or relates to a task carried out in the public interest (e.g. the processing of CCTV data may rely on the school's legitimate interest in maintaining a safe and secure school building). The school must demonstrate compelling legitimate grounds if such processing is to continue.
- 1.9 **Right not to be subject to automated decision making** This right applies in specific circumstances (as set out in GDPR Article 22).
- 1.10 **Right to withdraw consent** In cases where the school is relying on consent to process your data, you have the right to withdraw this at any time, and if you exercise this right, we will stop the relevant processing.
- 1.11 **Limitations on Rights** While the school will always facilitate the exercise of your rights, it is recognised that they are not unconditional: the school may need to give consideration to other obligations.<sup>2</sup>
- 1.12 **Right to Complain**
  - (i) If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Principal who is responsible for operational oversight of this policy.<sup>3</sup>
  - (ii) A matter that is still unresolved may then be referred to the school's Data Controller (i.e., the Board of Management) by writing to the Chairperson c/o school.
  - (iii) Should you feel dissatisfied with how we have addressed a complaint or concern that you have raised, you have the right, as data subject, to bring the matter to the attention of the Irish Data Protection Commission.

## 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.

<sup>2</sup> See GDPR Articles 12-23 for a full explanation of subject rights and their application.

<sup>3</sup> Parents/Guardians may also, where applicable, have the option of invoking the school's formal complaints procedure (available from school).



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

Name	Responsibility
Board of Management:	Data Controller
Principal:	Implementation of Policy, <b>Data Protection Co-ordinator</b>
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

#### Data Use

Personal data is at often at the greatest risk of loss, corruption, or theft when it is being used or accessed:

To mitigate this risk :-

- when working with personal data, all personnel will ensure that the screens of their computers/tablets/apps are always locked when left unattended.
- personal data shared by email will be downloaded, stored securely, and then deleted.
- data will be encrypted before being transferred electronically where appropriate.
- staff will not save copies of personal data to their own computers.

#### Sanctions and Disciplinary Action

Given the serious consequences that may arise Blackrock College may invoke appropriate disciplinary procedures for failure to adhere to the College's policy on Data Protection.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

#### Dealing with a Data Access Requests

Under Article 15 of the GDPR, 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.

Prior to complying with a Subject Access Request, we require proof of the applicant's identity and address to ensure that personal information is not given to the wrong person. Information requested will be provided by the College **within one month** of the identity of the individual of the data subject being verified.

In the normal course of events, the College is obliged to respond to your access request within one month of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). Where the College is extending the period for replying to your request, it must inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.

There is no fee payable by you to make an access request - the College will deal with your request for free. However, where the College believes a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the College may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s).

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.

For more detailed information please see Data Subject Access Policy on our website and Appendix 6.

#### Exceptions to the Right of Access

Article 15 of the GDPR also provides that the right to obtain a copy of personal data must not adversely affect the rights and freedoms of others. For example, the College will not provide the requestor with personal data relating to a third party that would reveal the third party's identity.



## 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.

## Data Access Request Handling Procedure

The General Data Protection Regulation (EU) 2016/679 provides for a right of access by an individual data subject to personal information held by Blackrock College. A person seeking information, the Data Subject, is required to familiarise himself/herself with this policy. This may apply to a staff member or student seeking information on his or her own behalf or maybe a parent/guardian seeking information on behalf of his or her own son. No information will be supplied that relates to another individual. Although from time to time an individual may request by telephone details of some elements of their personal data, formal **Data Subject Request** must be submitted in writing, either electronically or by post.

For more detailed information please see Data Subject Access Policy on our website.

## Students Making Access Requests

The right of access under Article 15 of the EU GDPR is the right of the data subject.

If the data contains health data and disclosure would be likely to cause serious harm to the physical or mental health of the individual concerned, the College is obliged to withhold the data until they have consulted with the data subject's medical practitioner and (in the case of a student under 18 or a student with special educational needs whose disability or medical condition would impair his or her ability to understand the information), parental/guardian consent should also be sought.

Each student request for Access to Personal Data will be assessed individually.

For more detailed information please see Data Subject Access Policy on our website.

## Parents Making Access Requests on Behalf of Their Son

Where a parent/guardian makes an access request on behalf of their child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the child is registered on the College's records and will be addressed to the child. The documentation will not be sent to or addressed to the parent/guardian who made the request.

For more detailed information please see Data Subject Access Policy on our website.

## Others Making an Access Request

On making an access request, any individual about whom the College keeps *Personal Data*, is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under GDPR apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing his/her data
- know the identity (or the categories) of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest
- where the processing is by automated means (e.g. credit scoring in financial institutions where a computer program makes the "decision" as to whether a loan should be made to an individual based on his/her credit rating) know the logic involved in automated decisions.

For more detailed information please see Data Subject Access Policy on our website.



### Steps in Making a Data Subject Request

1. The Data Subject applies in writing requesting access to his/her data. The school reserves the right to request official proof of identity (e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification
2. On receipt of the Data Access Request, the Principal will check the validity of the access request and check that sufficient information to locate the data requested has been supplied. It may be necessary for the Principal to contact the data subject in the event that further details are required with a view to processing the access request.
3. The Principal will ensure that all relevant manual and soft files are checked for the data in respect of which the access request is made.
4. The Principal will ensure that the information is supplied promptly and within one month of first receiving the request.
5. If data relating to a Third Party is involved, it will not be disclosed without the consent of that Third party or alternatively the data will be anonymised in order to conceal the identity of the third party. Where it is not possible to anonymise or conceal the identity of the third party the data to ensure that the Third Party is not identified, then that item of data may not be released.
6. Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.
7. The documents supplied will be numbered where appropriate.
8. Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

### Appealing a Decision in Relation to a Data Access Request

The Board of Management of Blackrock College is respectful of the right of the Data Subject to appeal a decision made in relation to a request for data from this school. To appeal a decision, the Data Subject is advised to write to or email the Data Protection Commissioner explaining the case:-

Canal House, Station Road, Portarlinton, Co. Laois

(info@dataprotection.ie)

The correspondence should include

- the name of the school
- the steps taken to have concerns dealt with
- details of all emails, phone calls, letters between the Data Subject and this College.

### Data Erasure and Disposal

When documentation or computer files containing personal data are no longer required, the information will be disposed of carefully to continue to ensure the confidentiality of the data.

When the purpose for which the information was obtained has ceased and personal information is no longer required, the data will be deleted or disposed in a secure manner according to Records Retention Schedule (see Appendix 1).

Paper-based files and information no longer required, will be safely disposed of in shredding receptacles. Usually the data will be shredded on site by school personnel – but occasionally a third party data destruction specialist will be employed and vetted staff will collect documents which will be shredded on site by the specialists.

In the case of personal information held electronically, temporary files containing personal information will be reviewed regularly and deleted when no longer required.

When personal data reaches the point where the retention period has expired, the information will also be securely deleted and removed. In the event that IT equipment containing personal data is no longer required, all data stored on the devices will be removed prior to disposal.

## **Data Breaches**

Definition: A data breach is an incident in which personal data has been lost, accessed, and/or disclosed in an unauthorised fashion.

This would include, for instance, loss or theft of a laptop containing staff or student details, an email with personal information being sent to the wrong recipient, as well as more organised incidents of external hacking.

All school personnel have a responsibility to take immediate action if there is a data breach.

For more detailed information please see Data Breach Policy on our website.

## **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 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.

## **Links to Other Policies/Code of Practices**

The College policies need to be consistent with one another. 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:

- CCTV Policy
- Data Access Request Policy
- Data Breach Policy
- Child Safeguarding Statement
- Anti-Bullying Policy
- Code of Behaviour
- Admissions/Enrolment Policy
- Substance Use Policy
- Acceptable Use Policy



## Reviewing and Evaluating the policy

On-going review and evaluation takes place based on 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 should be revised as necessary in the light of such review and evaluation and within the framework of College planning.

Signed: .....


*For and behalf of Board of Management*

Date: .....

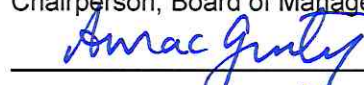
Data Protection Policy: May 2019

This policy has been ratified by the Board of Management on 20.08.19.

Signed:

  
Chairperson, Board of Management

Signed:

  
Secretary, Board of Management



# APPENDICES

## Appendix 1 - Records Retention Schedule

Student Records	Vol Sec.	Final disposition	Comments
Attendance Records	Indefinitely	N/A	Indefinitely. Archive when class leaves + 2 years
State exam results	N/A	N/A	SEC responsibility to retain, not a requirement for the College

Records relating to pupils/students	Vol Sec.	Confidential shredding	Comments
These records include: Application forms, Enrolment forms, Scholarship applications, Student transfer forms, Disciplinary notes, Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results), End of term/year reports, Records of school tours/trips, including permission slips, itinerary reports, Gaeltacht, book rental scheme	25 years after a student leaves the College	Confidential shredding	



Sensitive Personal Data Students	Vol Sec.	Final disposition	Comments
Psychological assessments	Indefinitely	N/A - Never destroy	Never destroy
Additional Educational Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	N/A	Never destroy
Students' medical records (i.e. nurses' roll books, boarders' individual files)	Student reaching 18 years + 2 years	Confidential shredding	
Accident reports	Indefinitely	N/A	Never destroy
Child protection records	Indefinitely	N/A	Never destroy
Section 29 appeal records	Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Enrolment/transfer forms where child is not enrolled or refused enrolment	Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Records of complaints made by parents/guardians	Depends entirely on the nature of the complaint.	Confidential shredding or N/A, depending on the nature of the records.	Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy.  If it is a complaint of a more mundane nature (e.g. misspelling of child's name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then student reaching 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)

Parents' Personal Data	Vol Sec.	Final Disposition	Comments
Names and addresses of parents/legal guardians, occupation and their contact details (including any special arrangements with regard to guardianship, custody or access); religious belief, place of work	25 years after a student leaves the College	Confidential shredding	
Financial information and fees correspondence	7 years, unless there are outstanding fees due or another family member is still a pupil on campus. All the information will be disposed 7 years after the last member of the family leaves the campus or the outstanding balance is discharged	Confidential shredding	



Unsuccessful Candidates for Interview	Vol Sec.	Final disposition	Comments
Applications & CVs of candidates called for interview		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Database of applications		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Selection criteria		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Applications of candidates not shortlisted		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Unsolicited applications for jobs		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Candidates shortlisted but unsuccessful at interview		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Candidates shortlisted and are successful but do not accept offer		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Interview board marking scheme & board notes		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.
Panel recommendation by interview board		Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Workplace Relations Commission to inform the school that a claim is being taken.

Staff personnel files	Vol.Sec	Final Disposition	Comments
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.		Confidential shredding. Retain an anonymised sample for archival purposes.	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Application &/CV		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Qualifications		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
References		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview: database of applications (the section which relates to the employee only)		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Selection criteria		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview board marking scheme & board notes		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Panel recommendation by interview board		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)



Force Majeure leave		Confidential shredding	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Carers leave		Confidential shredding	Must be kept for 8 years - Carer's Leave Act 2001  Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years
Working Time Act (attendance hours, holidays, breaks)		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). There is a statutory requirement to retain for 3 years
Allegations/complaints		Confidential shredding	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). <b>Please note</b> the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.
Grievance and Disciplinary records		Confidential shredding	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). <b>Please note</b> the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.

Occupational Health Records	Vol Sec.	Confidential Shredding	Comments
Sickness absence records/certificates		Confidential shredding Or N/A (see comment)	Re sick leave scheme (1 in 4 rule) ref DES C/L 0060/2010  Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Pre-employment medical assessment		Confidential shredding Or N/A (see comment)	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Occupational health referral		Confidential shredding Or N/A (see comment)	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Correspondence re retirement on ill-health grounds		Confidential shredding Or N/A (see comment)	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Accident/injury at work reports		Confidential shredding	Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy).
Medical assessments or referrals		Confidential shredding Or N/A (see comment)	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless Medmark assessment relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.



Sick leave records (sick benefit forms)		Confidential shredding	In case of audit/refunds, Current year plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
---	--	------------------------	---

Superannuation /Pension /Retirement records	Vol Sec.	Final Disposition	Comments
Records of previous service (incl. correspondence with previous employers)		N/A	DES advise that these should be kept indefinitely.
Pension calculation		Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Pension increases (notification to Co. Co.)		Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Salary claim forms		Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Government returns	Vol Sec.	Final disposition	Comments
Any returns which identify individual staff/pupils,		N/A	Depends upon the nature of the return. If it relates to pay/pension/benefits of staff, keep indefinitely as per DES guidelines. If it relates to information on students, e.g. October Returns, Annual Census etc., keep in line with "Student Records" guidelines above.

Board of Management Records	Vol Sec.	Final disposition	Comments
Board agenda and minutes		N/A	Indefinitely. These should be stored securely on school property
School closure			On school closure, records should be transferred as per <u>Records Retention in the event of school closure/amalgamation</u> . A decommissioning exercise should take place with respect to archiving and recording data.
Other school based reports/minutes	Vol Sec.	Final disposition	Comments
CCTV recordings		Safe/secure deletion.	60 days in the normal course, but longer on a case-by-case basis e.g. where recordings/images are requested by An Garda Síochána as part of an investigation or where the records /images capture issues such as damage/vandalism to school property and where the images/recordings are retained to investigate those issues.
Principal's monthly report including staff absences		N/A	Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".
Financial Records	Vol Sec.	Final disposition	Comments
Audited Accounts		N/A	Indefinitely
Payroll and taxation			Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection.
Invoices/back-up records/receipts			Retain for 7 years



Promotion process	Vol Sec.	Final Disposition	Comments
Posts of Responsibility		N/A	Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)
Calculation of service		N/A	Retain indefinitely on master file
Promotions/POR Board master files		N/A	Retain indefinitely on master file
Promotions/POR Boards assessment report files		N/A	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents		N/A	Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.
Correspondence from candidates re feedback		N/A	Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.

## Appendix 2. Glossary

**Child** - a person under the age of 18 years. Children are deemed as vulnerable under GDPR and merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

**Controller or Data Controller** - an entity or person who, alone or jointly with others, determines the purposes and means of the processing of personal data. In this policy, the data controller is the College.

**Consent** - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Data Protection Commission** - the national supervisory authority responsible for monitoring the enforcing the data protection legislation within Ireland. The DPC is the organisation to which Colleges as data controllers must notify data breaches where there is risk involved.

**Data Protection Legislation** – this includes (i) the General Data Protection Regulation (GDPR) - *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and (ii) the Irish Data Protection Act (2018). GDPR is set out in 99 separate *Articles*, each of which provides a statement of the actual law. The regulation also includes 171 *Recitals* to provide explanatory commentary.

**Data Subject** - a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

**Data concerning health** - personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. This is an example of special category data (as is data concerning special education needs).

**Personal data** - any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Personal data breach** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Processing** - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Processor or Data Processor** - a person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract (but does not include an employee of a controller who processes such data in the course of his or her employment).

**Profiling** - any form of automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

**(Relevant) Filing System** - any set of information that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

**Special categories of data** - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.



## Appendix 3. Personal Data and Related Processing Purposes

PURPOSES FOR PROCESSING	DESCRIPTION OF PERSONAL DATA
<b>1. Contact and identification information</b> This information is needed to identify, contact and enrol students.	
Purposes may include: <ul style="list-style-type: none"> <li>• to add names to a contact list prior to formal application</li> <li>• to provide appropriate information to prospective students</li> <li>• to make contact in case of College closure (e.g. adverse weather conditions)</li> <li>• to send SMS text messages and emails about meetings, etc.</li> </ul>	Information required to confirm student/parent identity and contact through communications: <ul style="list-style-type: none"> <li>• student name</li> <li>• gender</li> <li>• date of birth</li> <li>• family details (parents/guardians name, address, contact details to include phone numbers, email addresses etc).</li> </ul>
<b>2. Application information</b> We use this to determine whether an applicant meets eligibility requirements as set out in our Admission Policy.	
In addition to data outlined at (1) above, we collect personal data via Application Forms and Student Transfer Forms. Where the student is offered a place, completed Application Forms are placed on the student's file. Where the student is not offered a place, the data will be used for the purposes of responding to any section 29 appeals process.	Information as required to ascertain eligibility under the College's Admissions Policy: <ul style="list-style-type: none"> <li>• Name and address of current College</li> <li>• Class in current College</li> <li>• Details of siblings, etc.</li> <li>• Details of any special educational needs (SEN). (NB <u>only</u> for admission to a special College, or a SEN unit).</li> <li>• Language: details re Irish language. (Gaelscoil / Gaelcholáiste only)</li> </ul>
<b>3. Enrolment information</b> Once the College has accepted the student's application, and has offered the student a place, other information is collected in addition to the data outlined at (1) and (2) above. This personal data is used for administrative and management tasks e.g. College communications, timetabling, scheduling parent teacher meetings, College events, arrangements for academic registration, class details, start dates, book lists, subject-selection, College trips etc.	
<u>Contact and Identification Information:</u> We use this information: <ul style="list-style-type: none"> <li>• to make contact in case of College closure (e.g. adverse weather conditions), or an emergency (ill-health or injury),</li> <li>• to communicate issues relating to progress, welfare or conduct in College, non-attendance or late attendance, etc.</li> <li>• to send SMS text messages and emails about important events, e.g. start dates, course details, meetings, College events, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Student name and date of birth (requires birth certificate verification by College)</li> <li>• PPSN, Address including Eircode</li> <li>• Extended family details (parent/guardian names, contact details, postal &amp; email address, phone numbers, addresses, details of any court orders or other arrangements governing access to, or custody of, child).</li> <li>• Details of next of kin (for contact in case of emergency)</li> </ul>
<u>Academic record:</u> We use this information to deliver education appropriate to the needs of the student, to assess the student's educational progress. Standardised test results used for the purposes of assessing literacy/numeracy progress, for Reasonable Accommodation in State Examinations, for assisting in referrals to NEPS, and for career guidance etc.	<ul style="list-style-type: none"> <li>• Reports, references, assessments and other records from any previous College(s) attended by the student.</li> <li>• Education Passport (6<sup>th</sup> Class Report provided by primary College <u>after post-primary College confirms enrolment</u>. Protocols set out in DES Circulars 42/2015 and 34/2016).</li> <li>• Standardised testing Results</li> </ul>
<u>Language spoken:</u> Without this information the College will not know how to meet the student's needs and to deliver appropriate education. This ensures the student has access to language support (where necessary).	<ul style="list-style-type: none"> <li>• Information about language spoken (for language support)</li> <li>• Details of whether the student received EAL</li> </ul>



<p><u>Irish Exemption</u> Information re application for Irish exemption if eligible (e.g. received primary College up to 11 years of age outside Ireland, evidence of disability, student from abroad etc).</p>	<p>(English as an Additional Language) support.</p> <ul style="list-style-type: none"> <li>• Details re whether student is exempt from studying Irish</li> <li>• Details to ascertain if student is eligible for exemption from study of Irish</li> </ul>
<p><u>Medical information for health purposes:</u> This information is essential to meet our duty of care to the student. We use this information to (i) ensure we know who to contact in case of emergency, (ii) ensure that we have relevant information to safeguard/prevent damage to student health (iii) meet medical/care needs when students are in College (iv) facilitate appropriate advanced planning with parents/guardians (e.g. notification to relevant personnel within the College, storage of medications, staff training where necessary etc).</p>	<ul style="list-style-type: none"> <li>• Emergency contact details (name, telephone, details of relationship to the student etc).</li> <li>• Details of the student's GP (to be contacted in case of emergency).</li> <li>• Details of any relevant medical information (e.g. medical condition, allergies, treatment/care plan etc) to facilitate appropriate advanced planning with parents/guardians. This may include use of student's photograph for display in the Staff room as part of the emergency action plan.</li> </ul>
<p><u>SEN and Medical information for educational purposes:</u> We cannot meet our duty of care to the student and our obligations under EPSEN Act 2004 without this information. We use this information to (i) make application to the DES for allocation of resources to support student (ii) ensure College has relevant information to deliver education appropriate to student's needs (iii) apply for appropriate accommodation(s) and/or therapeutic supports where available.</p>	<ul style="list-style-type: none"> <li>• Details of any special needs/medical needs that need to be accommodated, e.g. medical assessment, hearing/vision issues, psychological assessment/report.</li> <li>• Details of whether the student has been in receipt of learning support.</li> <li>• Details of whether the student been granted resource teaching hours and/or special needs assistance hours by the NCSE.</li> </ul>
<p><u>Information sought by Department of Education and Skills (DES):</u> We are under a legal obligation to return specific enrolment information concerning each student to DES (SI 317/2015). This data is used to calculate teacher and resource allocation, capitation, grant payments for Colleges, for statistical analysis and reporting in the areas of social inclusion and integration of students in the education system, and for planning purposes. Other (optional) information is sought for purposes relating to planning, social inclusion and integration of students in the education system.</p>	<p>Personal data is transferred to the DES via the Post-Primary Online Database as set out in the <u>Privacy Notice for P-POD</u> provided by DES. Required information includes, e.g. birth name of student and mother (to verify student identity). The DES seeks some additional information on an optional basis (i.e. based on parental consent), for example,</p> <ul style="list-style-type: none"> <li>• Ethnic/Cultural background</li> </ul>
<p><u>Use of photographs for yearbooks, social media, website etc.:</u> Photographs, and recorded images of students may be taken at College events and to celebrate College achievements, compile yearbooks, establish a College website, record College events, and to keep a record of the history of the College.</p>	<ul style="list-style-type: none"> <li>• Consent to use (for these purposes) images or recordings in printed or digital format.</li> <li>• Separate consents will be sought for different publication forums. (NB This <u>excludes</u> CCTV recordings - see College CCTV policy).</li> </ul>
<p><b>4. Personal data gathered during student's time in College</b> We cannot meet our statutory obligation to deliver appropriate education to students and/or we cannot satisfy our duty of care to each student without processing this information.</p>	
<p><u>Academic progress:</u> The College processes this personal data in order to deliver education to students, and to evaluate students' academic progress, to register the student for State Examinations (Junior Cycle, Leaving Cycle), to submit the students' work to the recognised accrediting body etc.</p>	<ul style="list-style-type: none"> <li>• Academic progress and results</li> <li>• State exam results</li> <li>• Results of in-College tests/exams (i.e. end of term, end of year exams, assessment results)</li> <li>• Continuous assessment and end of term/year reports</li> </ul>
<p><u>Attendance:</u> The College is required to collect and monitor attendance data and to notify the Education Welfare Officer (TUSLA) in certain circumstances, such as (i) where the student is suspended for 6 days or more (ii)</p>	<p>Statutory processing pursuant to the Education (Welfare) Act 2000.</p> <ul style="list-style-type: none"> <li>• Attendance records including Registers and Roll books etc.</li> </ul>



where the student is absent for an aggregate period of 20 College days during the course of the year, (iii) where the Principal is of the opinion that the student is not attending College regularly. The College will notify parent/guardian in the event of non-attendance or absences.	<ul style="list-style-type: none"> <li>Records of referrals to TUSLA</li> </ul> <p>College Register and Roll Books are documents of enduring historical value and are retained in the College's archives for archival purposes in the public interest.</p>
<u>College tours/trips:</u> Information required to make appropriate travel arrangements, to implement insurance cover, to arrange appropriate supervision ratios, to ensure medical/health issues are properly accommodated, to engage in responsible planning, and to ensure necessary paperwork for INIS (Irish Border Control/Irish Naturalisation & Immigration Service requirements where children are travelling with someone other than their parent or guardian).	<p>Information to ensure trip is properly organised and supervised, including:</p> <ul style="list-style-type: none"> <li>permission slips (signed by parents/guardians),</li> <li>itinerary reports</li> <li>Letter from parent(s)/guardian(s) giving consent to travel.</li> <li>Copy of birth/adoption certificate or guardianship papers</li> <li>Copy of marriage/divorce certificate (where parent has different surname to child).</li> <li>Copy of the parent/guardian's passport or State identity document.</li> </ul>
<u>Garda vetting outcomes:</u> Certain work experience roles may require that a student be Garda vetted (Statutory vetting process).	<p>Information as set down in National Vetting Bureau (Children and Vulnerable Persons) Act 2012.</p> <ul style="list-style-type: none"> <li>Garda vetting form</li> </ul>
<u>CCTV images:</u> The College processes this data for the purposes outlined in our CCTV Policy, a copy of which is available on the College's website e.g. <i>We use CCTV for security purposes; to protect premises and assets; to deter crime and anti-social behaviour; to assist in the investigation, detection, and prosecution of offences; to monitor areas in which cash and/or goods are handled; to deter bullying and/or harassment; to maintain good order and ensure the College's Code of Behaviour is respected; to provide a safe environment for all staff and students; for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and the recordings may be capable of resolving that dispute; for the taking and defence of litigation.</i>	<p>CCTV is in operation at the perimeter, exterior and certain internal common areas within the College both during the daytime and during the night hours each day. CCTV is used at external points on the premises (e.g. at front gates, in the car-park etc) and at certain internal points (e.g. front desk/reception area, corridors etc). In areas where CCTV is in operation, appropriate notices will be displayed.</p>
<u>Special needs data, educational support records, medical data etc:</u> Without this information, the College will not know what resources need to be put in place in order to meet the student's needs and to deliver appropriate education in-keeping with its statutory obligations. This is in order to assess student needs, determine whether resources can be obtained and/or made available to support those needs, and to develop individual education plans. 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 (the statutory agency established under the Education for Persons with Special Educational Needs Act 2004) such information as the Council may from time to time reasonably request.	<p>The College collects information relating to any special educational needs, psychological assessments/reports, information about resource teaching hours and/or special needs assistance hours, etc. Colleges are also required to share this personal data with SENOs employed by the NCSE.</p> <ul style="list-style-type: none"> <li>Psychological assessments,</li> <li>Special Education Needs' files, reviews, correspondence</li> <li>Individual Education Plans,</li> <li>Learning support file,</li> <li>Notes relating to inter-agency meetings,</li> <li>Medical information (including details of any medical condition and/or medication/treatment required)</li> <li>Psychological, psychiatric and/or medical assessments</li> </ul>
<u>Child protection, child welfare records:</u> The College is required to follow DES Child Protection Procedures (Circular 81/2017) and to take appropriate action to safeguard the welfare of students in its care (Child	<p>Mandatory reporting obligations require data sharing with TUSLA, An Garda Síochána and any other appropriate law enforcement or child protection authorities. DES Inspectorate may</p>



Protection Procedures for Primary and Post-Primary Colleges 2017). Staff have a legal responsibility to report actual or suspected child abuse or neglect to the Child & Family Agency ("TUSLA") and to An Garda Síochána. Mandatory reporting obligations arise under Children First 2015, the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012.	<p>seek access to the College's child protection records for audit purposes.</p> <ul style="list-style-type: none"> <li>• Child protection records</li> <li>• Child safeguarding records</li> <li>• Other records relating to child welfare</li> <li>• Meitheal meetings convened by TUSLA</li> </ul>
<u>Counselling &amp; Pastoral Care Records:</u> This information is required to provide access to counselling services and/or psychological services and to provide supports to students, resolve behavioural, motivational, emotional and cognitive difficulties through assessment and therapeutic intervention, to engage in preventative work etc. Personal data (and special category personal data) will be shared with third parties (e.g. TUSLA, NEPS, CAMHS, An Garda Síochána, Medical practitioners treating the student) for the purpose of the College complying with its legal obligations and/or in the student's vital/best interests.	<ul style="list-style-type: none"> <li>• Guidance Counselling notes</li> <li>• Psychological service notes</li> <li>• Referrals to/records relating to therapeutic services and other interventions</li> <li>• Minutes, notes and other records concerning Student Support Team/Pastoral Care Team Meetings</li> </ul>
<u>Internal College processes:</u> This information (e.g. anti-bullying processes and disciplinary/Code of Behaviour processes) is required to meet the College's duty of care to all its students and staff, to comply with relevant Circulars issued by the Department of Education and Skills, and to run the College safely and effectively. Data collected in these processes may be transferred to the College's insurer and/or legal advisors or management body as appropriate where required for disputes resolution, fact verification, and for litigation purposes.	<ul style="list-style-type: none"> <li>• Records of parental complaints.</li> <li>• Records of other complaints (student to student complaints etc).</li> <li>• Records relating bullying investigations.</li> <li>• Records relating to Code of Behaviour processes (expulsion, suspension etc.) including appeals data and section 29 appeals material.</li> </ul>
<u>Accident and injury reports:</u> This information is processed to operate a safe environment for students and staff, to identify and mitigate any potential risks, and to report incidents/accidents. This data may be transferred to the College's insurance company and/or indemnifying body and/or legal advisors as appropriate. Data will be shared with An Garda Síochána, TUSLA and the Health & Safety Authority where appropriate.	<ul style="list-style-type: none"> <li>• Accident reports</li> <li>• Incident Report Forms</li> <li>• Notifications to insurance company</li> <li>• Exchanges with legal advisors.</li> <li>• Notifications to Health &amp; Safety Authority (HSA)</li> </ul>
<u>Financial information, fees etc:</u> Without this information, the College cannot process applications, make grant payments, or receive payment of monies (e.g. course fees, College trips etc). After completion of the payments, the documentation is retained for audit and verification purposes. The College's financial data are audited by external auditors.	<ul style="list-style-type: none"> <li>• Information relating to payments from student's parents/guardians (including fee support and fee waiver documentation),</li> <li>• Scholarship/Grant applications (including Gaeltacht, book rental scheme etc).</li> </ul>
<b>5. Parent Nominees on Boards of Management</b> This information is required to enable the Board of Management to fulfil its statutory obligations.	
Processing undertaken in accordance with the Education Act 1998 and other applicable legislation, including decisions taken for accountability and good corporate governance.	<ul style="list-style-type: none"> <li>• Name, address and contact details of Parent Nominee</li> <li>• Records in relation to appointment to the Board</li> <li>• Minutes of Board of Management meetings and correspondence to the Board.</li> </ul>



## Appendix 4 – Categories of Recipients

**Department of Education and Skills (DES)** The College is required to provide student data to the *Department of Education and Skills (DES)*. This transfer of data is primarily made at the beginning of each academic year (“October Returns”) using a secure Post-Primary Online Database (P-POD) system. The October Returns contain individualised data such as PPS number which acts as an identifier to validate that the data belongs to a recognised student.<sup>4</sup> The DES has published a “Fair Processing Notice” to explain how the personal data of students is processed.<sup>5</sup>

**State Examinations Commission (SEC)** data on entrants for the state examinations is provided via the October Returns to SEC to assist its planning of the state examinations.

**Student support and welfare** student data may be shared with a number of public state bodies including *National Educational Psychological Service* (NEPS psychologists support Colleges and students); *National Council for Special Education* (the NCSE role is to support Colleges and students with special education needs); *National Education Welfare Board* (the College is required to share student attendance with the NEWB). Data to support student access to further and higher education may also be shared for processing as part of *Student Universal Support Ireland (SUSI)*, *Higher Education Access Route (HEAR)* and *Disability Access Education Route (DARE)*.

**Legal requirements** where appropriate, particularly in relation to Child Protection and safeguarding issues, the College may be obliged to seek advice and/or make referrals to *Tús/la*.<sup>6</sup> The College may share personal data with *An Garda Síochána* where concerns arise in relation to child protection. The College will also report matters of alleged criminal acts, criminal behaviour, criminal damage, etc., to allow prevention, detection and investigation of offences. Where there is a lawful basis for doing so, personal data may also be shared with the *Revenue Commissioners* and the *Workplace Relations Commission*.

**Insurance** data may be shared with the College's insurers where this is appropriate and proportionate. The College may also be obliged to share personal data with the *Health and Safety Authority*, for example, where this is required as part of an accident investigation.

**Professional Advisors** some data may be shared with legal advisors (solicitors, etc.), financial advisors (pension administrators, accountants, etc.) and others such as College management advisors; this processing will only take place where it is considered appropriate, necessary and lawful.

**Other Colleges and Universities/Colleges/Institutes** where the student transfers to *another educational body*, or goes on an exchange programme or similar, the College may be asked to supply certain information about the student, such as academic record, references, etc.

**Work Placement** some data may be shared, on request, with work placement providers and *employers* where this is appropriate and necessary to support students engaged in work experience or similar programmes.

**Other not-for-profit organisations** limited data may be shared with recognised bodies who act to promote student engagement with co-curricular and other activities, competitions, recognition of achievements, etc. This would include bodies promoting participation in sports, arts, sciences, environmental and outdoor activities, etc. This data sharing will usually be based on consent.

**Service Providers** in some circumstances the College has appointed third parties to undertake processing activities on its behalf. These Data Processors have provided guarantees that their processing satisfies the requirements of the General Data Protection Regulation. The College has implemented written contractual

<sup>4</sup> Where the October Returns include sensitive personal data regarding personal circumstances then explicit and informed consent for the transfer of this data may be sought from students/parents/guardians.

<sup>5</sup> These can be found on [www.education.ie](http://www.education.ie) (search for Circular Letters 0047/2010 and 0023/2016 in the “Circulars” section). The Department of Education and Skills transfers some student data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection & Employment Affairs 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.

<sup>6</sup> Tús/la, the Child and Family Agency, is the State agency responsible for improving wellbeing and outcomes for children.

agreements with these entities to ensure that the rights of data subjects receive an appropriate level of protection. Third party service providers include the following categories:

- College Management Information Systems (e.g. VSWare/Advanced)
- Productivity Applications (e.g. Google Apps for Education, Microsoft 365)
- Online Storage & File Sharing (e.g. Dropbox, Google Drive, iCloud, OneDrive)
- Video Sharing and Blogging Platforms (e.g. Youtube, Wordpress)
- Virtual Learning Environments (e.g. Edmodo, Collegeogy, Collegewise, Google Classroom)
- IT Systems Support (local ICT Support Company)
- Fee management software
- College communications
- Security and CCTV Systems
- Pension Consultants/Trustees
- Accounting & Payroll software
- Cashless Payment Systems
- Canteen Management System
- Learning software and Apps

**Transfers Abroad** In the event that personal data may be transferred outside the European Economic Area (EEA) the College will ensure that any such transfer, and any subsequent processing, is carried out in strict compliance with recognised safeguards or derogations (i.e., those approved by the Irish Data Protection Commission).



## Appendix 5 – Implementing the Data Processing Principles

### 1. Accountability

- (i) Accountability means that compliance with the data protection legislation is recognised as an important Board of Management responsibility as well as one shared by each College employee and member of the wider College community.<sup>7</sup>
- (ii) Demonstrating Compliance Accountability imposes a requirement on the controller to demonstrate compliance with the other data processing principles. This means that the College retains evidence to demonstrate the actions it has taken to comply with GDPR.
- (iii) College Policies An important way for the College to demonstrate accountability is through the agreement and implementation of appropriate policies. In addition to publishing a *Data Protection Policy* this may include developing other policies to address some or all of the following areas (i) CCTV<sup>8</sup> (ii) Data Breaches (iii) Data Access Requests (iv) Record Storage and Retention (v) Data Processing Agreements.<sup>9</sup>
- (iv) Record of Processing Activities As a data controller the College is required to prepare a record of any processing activities (ROPA) that it undertakes. This record should include the following information (GDPR Article 30):
  - the purposes of the processing;
  - a description of the categories of data subjects and personal data;
  - the categories of recipients to whom the personal data will be disclosed;
  - any transfers to a third country or international organisation, including suitable safeguards;
  - where possible, the envisaged time limits for erasure of the different categories of data;
  - where possible, a general description of the technical and organisational security measures.
- (v) Risk Assessment The College as data controller is required to consider any risks that may arise as a consequence of its processing activities. This assessment should consider both the likelihood and the severity of these risks and their potential impact on data subjects.<sup>10</sup>
- (vi) Data Protection Impact Assessment (DPIA) A DPIA is a type of risk assessment that is mandatory in specific circumstances (GDPR Article 35). The College will ensure that a DPIA is undertaken where this is appropriate, typically, where a new processing activity has the potential to have a high impact on individual privacy or rights. The purpose of undertaking a DPIA is to ensure that any risks associated with the new processing activity are identified and mitigated in an appropriate manner.
- (vii) Security of Processing As a consequence of having assessed the risks associated with its processing activities, the College will implement appropriate *technical and organisational measures* to ensure a level of security appropriate to the risk. For example, these measures might include training of staff, establishment of password policies, protocols around device encryption, procedures governing access to special category data etc.
- (viii) Data Protection by Design The College aims to apply the highest standards in terms of its approach to data protection. For example, College staff will utilise a *Privacy by Design* approach when any activity that requires the processing of personal data is being planned or

<sup>7</sup> The GDPR4schools.ie website identifies some of the GDPR Roles and Responsibilities held by different groups, namely (i) Board of Management (ii) Principal/Deputy Principal (iii) Teaching Staff (iv) Guidance & Medical Support (v) School Administration (vi) SNAs and (vii) Caretaker. These lists of responsibilities (provided in PDF format) can be shared out to help raise awareness amongst the school community.

<sup>8</sup> A template CCTV policy for Schools is available from [www.dataprotectionschools.ie](http://www.dataprotectionschools.ie).

<sup>9</sup> All school policies need to be applied in a manner that respects the principles, protocols and procedures inherent in the school's Data Protection strategy. Examples of relevant policies include (i) Acceptable Use Policy (ICT) (ii) Child Protection Procedures (iii) Code of Behaviour (iv) Guidance and Counselling (v) Policy on Special Education Needs (vi) Anti-Bullying Policy.

<sup>10</sup> GDPR Recital 75: The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.



reviewed. This may mean implementing technical measures (e.g. security) and organisational measures (e.g. protocols and training).

- (ix) Data Protection by Default A *Privacy by Default* approach means that minimal processing of personal data is the College's default position. In practice this means that only essential data will be collected from data subjects, and that within the College, access to this data will be carefully controlled and only provided to employees where this is appropriate and necessary.
- (x) Data Processing Agreements: the College will put written contracts in place with organisations that process data on its behalf (as required under GDPR Article 28).<sup>11</sup>
- (xi) Data Breach Records: the College will retain records that document its handling of any personal data breaches. These records will clearly set out the facts relating to any personal data breach, its effects and the remedial action taken.<sup>12</sup>
- (xii) Staff Awareness and Training All who are granted access to personal data that is under the control of the College have a duty to observe the data processing principles. The College will provide appropriate information, training and support so that staff may gain a clear understanding of these requirements.<sup>13</sup>

## 2. Lawful Processing

As part of its decision to collect, use or share personal data, the College as Controller will identify which of the lawful bases is applicable to each processing operation. In the absence of a lawful basis the personal data cannot be processed.

- (i) Many of College's data processing activities rely on legal obligations. These tasks are undertaken because the College must comply with Irish (or European) law<sup>14</sup>. For example, there is a legislative basis underpinning the sharing of specific student data with the Department of Education and Skills and other public bodies.
- (ii) Another set of data processing activities are undertaken in the public interest i.e. so that the College can operate safely and effectively. For example, an educational profile of the student (literacy competence, language spoken at home etc.) may help the College to target learning resources effectively for the benefit of the student.
- (iii) In some situations, for example the use of CCTV, the College may rely on its legitimate interests to justify processing. In such cases the specific legitimate interests (e.g. health and safety, crime prevention, protection of College property etc.) must be identified and notified to the data subjects<sup>15</sup>.
- (iv) Contract will provide a lawful basis for some processing of data by the College. For example, the processing of some employee data may rely on this lawful basis.
- (v) There is also the possibility that processing can be justified in some circumstances to protect the Vital Interests of a data subject, or another person. For example, sharing some data subject data with emergency services might rely on this lawful basis.
- (vi) Finally there is the option of using a data subject's consent as the lawful basis for processing personal data. The College will not rely on consent as the basis for processing personal data if another lawful condition is more appropriate. Consent will usually be the lawful basis used by the College to legitimise the publication of student photographs in print publications and electronic media.

---

<sup>11</sup> A Data Processing Agreement may be provided as a set of agreed clauses or as an addendum to a broader (*Third Party*) *Service Agreement*.

<sup>12</sup> These record-keeping requirements are detailed under GDPR Article 33(5). Documentation need to be retained in school setting out details of all data breaches that have occurred. This includes those that were adjudged not to require notification to the Data Protection Commission (in addition to data breaches that required formal DPC notification via <https://forms.dataprotection.ie/report-a-breach-of-personal-data>).

<sup>13</sup> All current and former employees of the school may be held accountable in relation to data processed by them during the performance of their duties. For example, employees acting in breach of the Data Protection Act 2018 could, in certain circumstances, be found to have committed a criminal offence.

<sup>14</sup> For example, the *Education Act 1998*, the *Education (Welfare) Act 2000* & the *Education for Persons with Special Education Needs Act 2004*.

<sup>15</sup> Data subjects have a right to object to processing that is undertaken based on legitimate interests. In such cases the Controller must demonstrate that there is an overriding need if the processing is to continue.



### 3. Consent

Where consent is relied upon as the appropriate condition for lawful processing, then that consent must be freely given, specific, informed and unambiguous. All of these conditions must be satisfied for consent to be considered valid. There are a significant number of restrictions around using consent.

- (vii) A separate consent will be sought for each processing activity (together with appropriate guidance as necessary to ensure the data subject is informed).
- (viii) When asking for consent, the College will ensure that the request is not bundled together with other unrelated matters.
- (ix) Consent requires some form of clear affirmative action (Silence or a pre-ticked box is not sufficient to constitute consent). Consent can be provided by means of an oral statement.
- (x) Consent must be as easy to withdraw as to give.
- (xi) A record should be kept of how and when consent was given.
- (xii) The College will take steps to ensure the consent is always freely given i.e. that it represents a genuine choice and that the data subject does not feel under an obligation to consent to processing.
- (xiii) If the consent needs to be explicit, this means the College must minimise any future doubt about its validity. This will typically require the College to request and store a copy of a signed consent statement.

### 4. Special Category Data

Some personal data is defined as Special Category Data and the processing of such data is more strictly controlled. In a College context this will occur whenever data that relates to Special Needs or Medical Needs is being processed. GDPR Article 9 identifies a limited number of conditions, one of which must be applicable if the processing of special category data is to be lawful.<sup>16</sup> Some of these processing conditions, those most relevant in the College context, are noted here.

- (xiv) Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law. This condition could provide an appropriate basis for processing of data relating to employee and student health e.g. proportionate sharing of special category data to ensure the College is compliant with provisions in health, safety and welfare legislation.
- (xv) Processing is necessary for the assessment of the working capacity of an employee;....or for the provision of health or social care or treatment.. on the basis of Union or Member State law.
- (xvi) Processing is based on Explicit Consent. Where a College is processing biometric data for identification purposes (e.g. facial image recognition or the use of fingerprint systems) it is unlikely that this processing will be justifiable on any lawful basis other than consent. (And, as a data subject should be able to withhold consent without suffering any detriment, the College will need to provide access to an alternative processing option which is not reliant on biometric data.)

### 5. Transparency

The College as Controller is obliged to act with *Transparency* when processing personal data. This requires the communication of specific information to individuals in advance of any processing of their personal data.<sup>17</sup>

- (i) Transparency is usually achieved by providing the data subject with a written document known as a *Privacy Notice* or a *Privacy Statement*.<sup>18</sup> This notice will normally communicate:
  - the name of the controller and their contact details;
  - the categories of personal data being processed;
  - the processing purposes and the underlying legal bases;
  - any recipients (i.e. others with whom the data is shared/disclosed);
  - any transfers to countries outside the EEA (and safeguards used);
  - the storage period (or the criteria used to determine this);

<sup>16</sup> The Data Protection Act 2018 makes provision for some additional conditions that can legitimise the processing of special category data.

<sup>17</sup> GDPR Articles 13 (or 14)

<sup>18</sup> Other terms in common use include *Fair Processing Notice* and *Data Protection Notice*. Schools may prepare a number of different Privacy Notices for use in different contexts. For example, a *Website Privacy Notice*, may relate specifically to personal data that is collected via the school website.



- the rights of the data subject.<sup>19</sup>
- (ii) Transparency information should be provided in a manner that is concise and easy to understand. To best achieve this, the College may use a “layering” strategy to communicate information.<sup>20</sup> And, while a written *Privacy Notice* is the default mode, transparency information may also be communicated using other means, for example through the spoken word or through use of pictorial icons or video.
- (iii) Privacy statements (include those used on College websites) should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data.

## 6. Purpose Limitation

- (i) Personal data stored by the College has been provided by data subjects for a specified purpose or purposes.<sup>21</sup> Data must not be processed for any purpose that is incompatible with the original purpose or purposes.<sup>22</sup>
- (ii) Retaining certain data (originally collected or created for a different purpose) with a view to adding to a College archive for public interest, scientific or historical research purposes or statistical purposes is acceptable subject to certain safeguards, most particularly the need to respect the privacy of the data subjects concerned.

## 7. Data Minimisation

As Controller, the College must ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In practice, this principle has a number of important implications illustrated in the examples below.

- (i) The College should ensure, when data is being collected from data subjects, that this is limited to what is necessary for the completion of the duties. For example, where information is being collected from students and parents/guardians, as part of the admissions process, this should be limited to whatever information is needed to operate the admissions process. This means that it is usually not appropriate for the College to seek information about Special Education Needs (SEN) in order to decide whether a place should be offered.<sup>23</sup>
- (ii) Data minimisation also requires that the sharing of student data within the College should be carefully controlled. Members of staff may require varying levels of access to student data and reports. Access should be restricted to those who have a defined processing purpose. Staff will not access personal data unless processing is essential to deliver on their role within the College.
- (iii) College staff will necessarily create personal data in the course of their duties. However employees should ensure that this processing is necessary and appropriate. For example, while it will often be necessary for College staff to communicate information to each other by email, consideration should be given, on a case by case basis, as to whether it is necessary for personal data to be included in these communications.
- (iv) Data sharing with external recipients should be continuously reviewed to ensure it is limited to that which is absolute necessary. This may mean, for example, that when the College is seeking professional advice, no personal data will be included in communications unless the disclosure of this information is essential.

<sup>19</sup> In the interests of transparency, the school should ensure that its preferred route for a rights request is identified clearly in *Privacy Notices* and elsewhere e.g. “A data subject wishing to make an access request should apply in writing to the Principal.” Notwithstanding this, school staff should be made aware that valid requests may be submitted in a variety of formats (i.e. not necessarily in writing).

<sup>20</sup> For example, where the first point of contact is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13 by way of further, different means, such as by sending a copy of the privacy policy by email and/or sending the data subject a link to the controller’s layered online privacy statement/notice.

<sup>21</sup> This purpose is usually communicated to data subjects at the time of collection through providing them with a *Privacy Notice*.

<sup>22</sup> Data Protection Commission: *Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.*

<sup>23</sup> SEN data may be sought where the processing of such data is necessary as part of the Admissions Policy. For example, SEN data may be required to consider whether the student fulfils the criteria for admission to a special education needs unit within a mainstream school.



## 8. Storage Limitation

Personal data is kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which it is being processed. Some personal data may be stored for longer periods insofar as the data is being processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- (i) When deciding on appropriate retention periods, the College's practices will be informed by advice published by the relevant bodies (notably the Department of Education and Skills, the Data Protection Commission, and the College management advisory bodies<sup>24</sup>).
- (ii) When documentation or computer files containing personal data are no longer required, the information is disposed of in a manner that respects the confidentiality of the data.
- (iii) Data subjects are free to exercise a "right to erasure" at any time (also known as the "right to be forgotten", see *Data Subject Rights*).
- (iv) Data should be stored in a secure manner that recognises controller obligations under GDPR and the Data Protection Act. This requires the College for example, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

## 9. Integrity and Confidentiality

Whenever personal data is processed by the College, technical and organisational measures are implemented to safeguard the privacy of data subjects. The College as controller is obliged to take its security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness. These security procedures should be subject to regular review.

- (i) College employees are required to act at all times in a manner that helps to maintain the confidentiality of any data to which they have access. Guidance and training are important to help identify and reinforce appropriate protocols around data security.
- (ii) The College is legally required to consider the risks to the data subject when any processing of personal data is taking place under its control. Any Risk Assessment should take particular account of the impact of incidents such as accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, the personal data.
- (iii) As well considering the potential severity of any data incident, a risk assessment should also consider the likelihood of any incident occurring. In this way risks are evaluated on the basis of an objective assessment, by which it is established whether the data processing operations involve a risk or a high risk.<sup>25</sup>
- (iv) The follow-on from any risk assessment is for the College to implement appropriate technical and organisational measures that ensure a level of security appropriate to the risk. *These measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected (GDPR Recital 83).*
- (v) As well as processing activities undertaken by staff, the College must also consider the risks associated with any processing that is being undertaken on behalf of the College by other individuals or organisations (Data Processors). Only processors who provide sufficient guarantees about the implementation of appropriate technical and organisational measures can be engaged.
- (vi) The important contribution that organisational policies can make to better compliance with the Accountability principle was previously highlighted. Similarly, the implementation of agreed policies and protocols around data security is very helpful. Some possible areas are listed below.
  - College ICT policy
  - Acceptable User Policies for employees, board members, students etc
  - Accessing College data from home

<sup>24</sup> see <http://www.dataprotectionschools.ie/en/Data-Protection-Guidelines/Records-Retention/>

<sup>25</sup> The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk (GDPR Recital 76).

- Password policy
- Use of staff personal devices in College
- Use of College devices outside College
- Bring Your Own Device Policy
- Social Media Policy
- Mobile phone code
- College use of Apps and Cloud Based Systems



## Appendix 6 – Managing Data Access Requests

### 1. Responding to rights requests

- i. The College will log the date of receipt and subsequent steps taken in response to any valid request. This may include asking the data subject to complete an *Access Request Form* in order to facilitate efficient processing of the request. There is no charge for this process.<sup>26</sup>
- ii. The College is obliged to confirm the identity of anyone making a rights request and, where there is any doubt on the issue of identification, will request official proof of identity (e.g. photographic identification such as a passport or driver's licence).<sup>27</sup>
- iii. If requests are manifestly unfounded or excessive<sup>28</sup>, in particular because of their repetitive character, the College may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to act on the request.
- iv. The College will need to confirm that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched<sup>29</sup>). Where appropriate the College may contact the data subject if further details are needed.
- v. In responding to rights requests (e.g. data access requests) the College will ensure that all relevant manual<sup>30</sup> and automated systems (computers etc.) are checked.
- vi. The College will be conscious of the need to respond without undue delay and within the advised timeframes. A response will be made within one month of receipt of any request.<sup>31</sup>
- vii. The College must be conscious of the restrictions that apply to rights requests.<sup>32</sup> Where unsure as to what information to disclose, the College reserves the right to seek legal advice.<sup>33</sup>
- viii. Where a request is not being fulfilled, the data subject will be informed as to the reasons and the mechanism for lodging a complaint, including contact details for the Data Protection Commission.
- ix. Where action has been taken by the College with regard to rectification, erasure or restriction of processing, the College will ensure that relevant recipients (i.e. those to whom the personal data has been disclosed) are appropriately informed.

### 2. Format of Information supplied in fulfilling a request

- i. The information will be provided in writing, or by other means, including where appropriate, by electronic means. (When requested by a data subject the information access may be provided in alternative means e.g. orally.)
- ii. The College will endeavour to ensure that information is provided in an intelligible and easily accessible format.
- iii. Where a request relates to video, then the College may offer to provide the materials in the form of a series of still images. If other people's images cannot be obscured, then it may not prove possible to provide access to the personal data.<sup>34</sup>

<sup>26</sup> The school may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information. Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

<sup>27</sup> Where a subject access request is made via a third party (e.g. a solicitor) the school will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement.

<sup>28</sup> In such circumstances, the school must be able to demonstrate the manifestly unfounded or excessive character of a request.

<sup>29</sup> The school will always endeavour to respond to any access request within the stipulated time period. However a timely response can be greatly facilitated by provided (in writing to the school) all necessary information such as date, time and location of any recording.

<sup>30</sup> Non-automated personal data that is held within a filing system or intended to form part of a filing system (GDPR Article 2).

<sup>31</sup> That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The school must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

<sup>32</sup> See for example GDPR Article 23 and Irish Data Protection Act 2018 S.56, S.60, S.61.

<sup>33</sup> Decisions around responding to data access requests will need to give due regard to rights and responsibilities that derive from other legislation, not least Article 42A of the Irish Constitution which recognises and affirms the natural and imprescriptible rights of all children. Examples of other factors that might need to be considered include: any court orders relating to parental access or responsibility that may apply; any duty of confidence owed to the child or young person; any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment); any detriment to the child or young person if individuals with parental responsibility cannot access this information; and any views the child or young person has on whether their parents should have access to information about them.

<sup>34</sup> Where an image is of such poor quality that it does not relate to an identifiable individual, then it may not be considered to be personal data.

## Appendix 7 – Reference Websites

Data Protection Act 2018 <http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html>

General Data Protection Regulation (GDPR official text) 2016 <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

General Data Protection Regulation (GDPR unofficial web version) 2016 <https://gdpr-info.eu/>

GDPR for school website <https://gdpr4schools.ie/>

Data Protection for Schools <http://dataprotectionschools.ie/en/>

Irish Data Protection Commission <https://www.dataprotection.ie/>

Data Breach Report <https://forms.dataprotection.ie/report-a-breach-of-personal-data>

European Data Protection Board (EDPB) <https://edpb.europa.eu/>

EDPB Guidelines, Recommendations and Best Practices on GDPR [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en)

DES Data Protection Page <https://www.education.ie/en/The-Department/Data-Protection/Information.html>

PDST Technology in Education <https://www.pdsttechnologyineducation.ie>

Cyber Security Centre (Ireland) <https://www.ncsc.gov.ie/>

Cyber Security Centre (UK) <https://www.ncsc.gov.uk/>