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).

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: Department of Finance, Principal Secretary's Office, Deputy Principal's Office, and Accommodation Manager'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 software ("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. 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 should be 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). See the template "Guidance on Taking and Using Images of Children in Schools"

- 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).

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" (see template)
- 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 and pastoral 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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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, State Examinations Commission, the Department of Social Protection, An Garda Síochána, the Health Service Executive, Tusla (CFA), 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.

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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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

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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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.

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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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 systems 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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section).

Purposes: The College asks parents/guardians and students to 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 should be able to access, alter, disclose or destroy personal data.
There is an automatic door and control system is 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.

Processing in Line with Data Subject's Rights

Data in this school will be processed in line with the rights of individuals as data subjects (Articles 12-23 of GDPR) and these rights are as follows:

• The right to have personal information processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
• The right to be informed, this means that the College needs to tell you what data we are using, why we are using it and for what purpose as well as informing you of the details of any third parties in receipt of data from the College.
• The right of access, you are allowed to see what data of yours we are processing if you request that from us.
• The right of rectification, that means if the data we are using is incorrect we have to correct it.
• The right to be forgotten, this means that we do not keep the data for a period longer than is necessary for the reason that it was originally collected. It also means that you have the right to issue a request to us requesting the erasure of your personal data. However, in many cases, the College will have overriding legitimate grounds for continued processing and will be unable to comply with such a request. This will be handled on a case by case basis, for further details please contact the College directly.
• The right to restrict processing, this means that you can ask us to stop using your data unless the College has a legitimate lawful purpose for continuing to do so.
• The right to data portability, this means that you have the right to move your data that you originally provided to the College to another data processor and the College has to provide you with this data in an acceptable format.
• The right to object, this means that you can object to the use of your data by the College and the College must stop using it unless it has an over-riding legitimate reason to continue.

Implementation Arrangements, Roles and Responsibilities

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

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

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

*****Please note the Principal's role is defined as **Data Protection Co-ordinator** previously referred as Data Protection Officer in Data Privacy Notice.

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.

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 files and computers 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, Portarlington, 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 Personal Data Breach Code of Practice 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 Procedures Policy
- Data Breach Code of Practice
- Child Safeguarding Statement
- Anti-Bullying Policy
- Code of Behaviour
- Mobile Phone Policy
- Admissions/Enrolment Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/CSPE etc.

Reviewing and evaluating the policy

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

This policy has been ratified by the Board of Management on 23.10.18

Signed: _____
Chairperson, Board of Management

Signed: _____
Chairperson, 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
Special Education Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	N/A	Never destroy
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)
Recruitment medical		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)
Job specification/ description		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)
Contract/Conditions of employment		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)

Probation letters/forms		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)
POR applications and correspondence (whether successful or not)		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)
Leave of absence applications		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)
Job share		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)
Career Break		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)
Maternity leave		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)
Paternity leave		Confidential shredding	Retain for 2 years following retirement/resignation 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).
Parental leave		Confidential shredding	Must be kept for 8 years - Parental Leave Act 1998 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.
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). **Please note** 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). **Please note** 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 Records Retention in the event of school closure/amalgamation. 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.	28 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.