St. Benildus College

Data Protection Policy and Procedures

RATIONALE

The characteristic spirit of St. Benildus 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 these aspirations and also the Data Protection Acts of 1988 and 2003, the General Data Protection Regulation of 2016 (GDPR- came into force 25/05/18)) 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.

The Board of Management of St. Benildus College is committed to the principles of responsible data protection as outlined in the documents referred to above and to this end it will:

- Obtain and fairly process personal data
- Keep data for one or more specified lawful purposes
- Process only data in ways compatible with the purposes for which it was given initially
- Securely store personal data
- Ensure that personal data is accurate and up-to-date
- Ensure that only relevant data is sought and stored
- Retain data no longer than is necessary for the specified purpose or purposes for which it was given
- Furnish a copy of personal data, or sensitive personal data to any individual, on request

Safeguarding Against Data Protection and Security Risks

This policy helps to protect the Board of Management of St. Benildus College from data security risks, including:

- **Breaches of security and confidentiality.** For instance, information being given out inappropriately.
- **Reputational damage.** For instance, the School could suffer if hackers successfully gained access to sensitive data.
- The risk of **large fines** or sanctions being imposed by the authorities.
- The **risks of being sued** for damages by individuals whose data has been mishandled.

Definitions as they pertain to this Policy

For the purpose of this policy the following definitions apply:

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.

Processing data refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

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.

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

- Racial or ethnic origin, political opinions or religious or philosophical beliefs
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Physical or mental health condition
- Sexual orientation

Data Controller refers to a person, company or body which determines the purposes and means of processing of personal data. The Data Controller for St. Benildus College is the Board of Management.

Wider Legal Obligations

The provisions of this policy take cognisance of the school's legal obligations and responsibilities in areas directly relevant to data protection, as outlined below:

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or in the case of a student who has reached the age of 18 years, the student, can have access in the prescribed manner to records kept by the school relating to the progress of the student in their education.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School.
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a relevant purpose.
- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs")) such information as the Council may from time to time reasonably request.
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished

information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body

- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Processing Personal Data

At St. Benildus College the personal data records sought and retained by the school may include but are not limited to those listed below:

A. Student Records:

It is the responsibility of parents/guardians to inform the school of any update to their son's data.

Categories of Student Data: These may include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. 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
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc.
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).
- Examination results including state examinations

The rationale for seeking and retaining student records is as follows:

- To enable each student to develop to his 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 son's educational progress
- To meet the educational, social, physical and emotional requirements of the student
- To celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school.
- To ensure that the student meets the school's admission criteria
- To ensure that students meet the minimum age requirements for their course.
- To ensure that any student seeking an exemption from Gaeilge/ Modern Foreign Language 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 (aged 13+) documentation/information/ references to third-level educational institutions and/or prospective employers

Student data is kept both in manual form, within a relevant filing system and on computer files. Computer files require a password and employees are required to maintain the confidentiality of any data to which they have access.

B. Staff records:

It is the responsibility of staff to inform the school of any update to their personal data.

Categories of Staff Data: These may include:

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

The rationale for seeking and retaining a staff member's personal data is as follows:

- To facilitate the management and administration of school business
- To facilitate the payment of staff, and calculate other benefits/ entitlements
- To facilitate pension payments in the future
- To manage human resources
- To record promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- To enable the school to comply with its obligations as an employer under the Safety, Health and Welfare at Work Act 2005
- To enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- For compliance with legislation relevant to the school.

Staff data is kept both in manual form, within a relevant filing system and on computer files. Computer files require a password and employees are required to maintain the confidentiality of any data to which they have access.

C. 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)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board that may include references to particular individuals.

The rationale for seeking and retaining Board of Management data is as follows:

- 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.
- Board of Management data is kept both in manual form, within a relevant filing system and on computer files. Computer files require a password and employees are required to maintain the confidentiality of any data to which they have access.

D Creditors/Debtors

Categories of Creditors/Debtors Data: These may include

- Name
- Address
- Contact details
- PPS number
- Tax details
- Bank details
- Amount paid
- Amount owed

The rationale for seeking and retaining a creditor's/debtors personal data is as follows:

- 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.

E October Returns

At the beginning of each academic year (and for 1st year or transferring students, on enrolment) parents/guardians and students are asked to provide the school with certain information so that the School can make returns to the Department of Education and Skills ("DES") referred to as "October Returns". These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The October Return contains individualised data (such as an individual student's PPS number) which acts as an identifier for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the

Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section).

The rationale for seeking and retaining personal data pertinent to October returns is as follows:

- October Returns are made in order to comply with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school.
- Personal data pertaining to October Returns is kept on computer files. Computer files are password protected and employees are required to maintain the confidentiality of any data to which they have access.

Responsibilities and Compliance

Everyone who works for or with St. Benildus College has responsibility for ensuring data is collected, stored, and handled appropriately. Each person who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Specific responsibilities are outlined in more detail below.

The Principal as Data Protection Officer (DPO) will

- Ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff induction, staff meetings and via the staff handbook.
- Ensure that there are regular updates to data protection awareness, so that data protection is a "living" process aligned to the school's ethos
- Periodically check data held regarding accuracy

The Board of Management as Data Controller will:

- Inform the person or persons involved, that a breach of confidentiality has occurred and that their personal data may have been compromised.
- Investigate where a breach of security has occurred and invoke appropriate action
- Review and update the Data Protection Policy if required.
- Ensure that only relevant data is processed
- Check to see if clerical and computer procedures are adequate to ensure accuracy.
- Reassure parents/guardians that the Data Protection Policy has been reviewed
- In tandem with the DPO, advise and inform employees of the need to work within the demands of the school's Data Protection policy.

St. Benildus College Staff as Data Processors will:

- Be required to sign off to confirm they have read and understand the Data Protection Policy and Procedures.
- Check that any information that they provide in connection with their employment is accurate and up to date.
- Notify the school of any changes to information they have provided, for example change of address.

- Ensure that personal information relating to students or their families is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.

Sanctions and Disciplinary Action

Given the serious consequences that may arise, St. Benildus College may invoke appropriate disciplinary procedures for failure to adhere to the school'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.

Compliance Monitoring and Review

St. Benildus College will undertake regular reviews of internal procedures and changes in the legislation to ensure ongoing compliance with General Data Protection Regulation. This will include an annual review.

Data Security - Overview

- Access to data will be restricted to authorised staff on a "need-to-know" basis and where it is needed to fulfill their duties and responsibilities.
- Data will not be shared informally.
- St. Benildus College will provide training to all staff to help them understand their responsibilities when processing data.
- Staff will keep all data secure by taking sensible precautions and following the guidelines below.
- Strong passwords will be used**,** and never shared.
- Personal data will not be disclosed to unauthorised people, either within St. Benildus College or externally.
- Data will be regularly reviewed and if found to be out of date, will be deleted or disposed of according to the guidelines below.
- Staff will request help from the DPO or Data Controller if they are unsure about any aspect of data protection.

Data Storage

The security of personal information relating to students and staff is a very important consideration under the Data Protection Acts and is taken very seriously at St. Benildus College . Appropriate security measures will be taken by the school to protect unauthorised access to this data and to the data it is collecting and storing on behalf of the Department of Education and Skills (DES).

A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised staff on a "need-to-know" basis.
- Manual files will be stored in a relevant filing system, located away from public areas.
- Computerised data will be held under password protected files.
- Any information which needs to be disposed of will be done so carefully and thoroughly.
- The premises at St. Benildus College are protected by Security and are monitored on a 24 hour/7 day week basis by Action 24 Security.

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it. This also applies to data that is usually stored electronically but has been printed out for a valid reason:

- When not required, the paper or files will be kept in a relevant filing system
- All personnel will ensure that personal data, paper and printouts are not left where unauthorised people could see them.
- Data will be shredded and disposed of securely when no longer required.

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (e.g. a USB key), these will be kept locked away (and ideally encrypted) when not being used.
- Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location.
- Data will be backed up frequently.
- All servers and computers containing data will be protected by an approved security software and a firewall.

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 sensitive personal data to their own computers.

Data Accuracy

St. Benildus College is cognisant of its duty to take reasonable steps to ensure that data is kept accurate and up-to-date.

- Data will be held in as few places as necessary.
- Every opportunity will be taken to ensure that data is updated (for example, by updating a student's contact information).
- St. Benildus College will make it as easy as possible for data subjects to update the information held about them, over the phone, or by email.
- Data will be updated as and when inaccuracies are discovered (for example), if a data subject can no longer be reached on their stored telephone number, it will be removed from the database.

Data Disclosure to Third Parties

As the Data Controller, the Board of Management is responsible for any personal data passed to third parties and care will be given to procedures and security.

The only data disclosed to third parties in the normal course of events is as described in St. Benildus College School Privacy Notices and Register of Personal Data Records.

The following list includes examples of such organisations but is not exhaustive:

- An Garda Síochána
- Túsla
- Department of Education and Skills
- Insurance Company
- Health and Safety Authority
- Workplace Relations Commission
- Revenue Commissioners

Note: Data Collected Through Garda Vetting

St. Benildus 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.

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.

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.

Subject Access Request (SAR) Handling Procedure

The Data Protection Acts, 1988 and 2003, the Data Protection Bill of 2018 and the 2016 GDPR provide for a right of access by an individual data subject to personal information held by St. Benildus 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 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 SARs must be submitted in writing, either electronically or by post.

Students making access requests

The Board of Management of St. Benildus College , in compliance with the GDPR recognises that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned, and also their rights in relation to the processing of personal data. It aims to balance the complementary rights of the child outlined in Articles 16(i) and 5 of the UN Convention of the Rights of the Child,

these being that “no child shall be subjected to arbitrary or unlawful interference with his and her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour” and “rights and duties of parents to provide……. in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognised in the present Convention”.

- A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- While a student aged from **thirteen up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that:
    - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
    - If the information is of a sensitive nature, parental/guardian consent will be sought before releasing the data to the student
    - If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student.
- Each student request for Access to Personal Data will be assessed individually.

Parents making access requests on behalf of their son

Where a parent/guardian makes an access request on behalf of his/her son (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 son, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the student is registered on the school’s records and will be addressed to the son / daughter subject to the provisions above.

Others making an access request

The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of the processing of their personal data. Under the GDPR and the current Data Protection Acts (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- The reasons why their data is being processed,
- The description of the personal data concerning them,
- Anyone who has received or will receive their personal data, and
- Details of the origin of their data if it was not collected from them.

To ensure SARs are responded to in a timely and effective manner, responsibility for identification and management of all requests will be assigned to a Designated Person. At St. Benildus College the Designated Person is the Principal and in his/her prolonged absence, the Deputy Principal.

Steps in Making a Subject Access Request (SAR)

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 log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.

4. 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.

5. The Principal will ensure that the information is supplied promptly and within one month of first receiving the request.

6. 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.

7. Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.

8. The Principal will ensure that the information is provided in an intelligible form (e.g. codes explained) where possible.

9. The documents supplied will be numbered where appropriate.

10. The Principal will sign off on the data supplied.

11. The school reserves the right to supply personal information to an individual in an electronic format e.g. on USB etc

12. 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 St. Benildus 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 this school
- The steps taken to have concerns dealt with
- Details of all emails, phone calls, letters between the Data Subject and this school.

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.

- If a staff member suspects at any time and for any reason that a breach may have occurred, then there is a need to report it to the DPO/Data Controller as an urgent priority
- Once notification of an actual or suspected breach has been received, the DPO/Data Controller will put the Data Breach Procedure into operation with immediate effect.

Data Breach Handling Procedure

The purpose of the Data Breach Procedure here below, is to ensure that all necessary steps are taken to:

(i) Contain the breach and prevent further loss of data

(ii) Ensure data subjects affected are advised (where necessary)

(iii) Comply with the law on reporting the incident to the Data Protection Commissioner if necessary

(iv) Learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future

Data Breach Response Plan

- A Breach Incident Leader will be nominated. This will typically be the DPO.
- Stakeholders will be identified
- A breach response handling team will be formed - comprising the school's Senior Management Team / the IT Coordinator / external IT supplier etc.
- The five-step process below will be initiated, with an evaluation after each stage

The information communicated to data subjects will include information on the nature of the personal data breach and a contact point where more information can be obtained. It will recommend measures to mitigate the possible adverse effects of the personal data breach.

The maximum timeframe for notification to the Office of the Data Protection Commissioner has been set at 72 hours from the time the incident is first discovered.

DATA BREACH – FIVE STEP PROCESS

1. **Identification and Initial Assessment of the Incident.**
    - Identify and confirm volumes and types of data affected
    - Establish what personal data is involved in the breach
    - Identify the cause of the breach
    - Estimate the number of data subjects affected
    - Establish how the breach can be contained

2. **Containment and Recovery**

- Establish who within the school needs to be made aware of the breach
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause
- Partial or complete systems lockdown
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual)

3. **Risk Assessment:**

   A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish

   - Risks for Data Subjects
   - Risks for St. Benildus College

4. **Notification**

   On the basis of the evaluation of risks and consequences, the Breach Response Team will decide whether it is necessary to signal the breach outside of the school. For example

   - The Gardaí
   - The Data Subjects affected by the breach
   - The Data Protection Commissioner
   - The school's insurers

In accordance with the Data Protection Commissioner's Code of Practice **all** incidents in which **Personal Data** has been put at risk will be reported to the Office of the DPC within 72 hours of St. Benildus College first becoming aware of the breach.

If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected **and** it affects no more than 100 Data Subjects **and** it does not include sensitive personal data or personal data of a financial nature, it may not require to be notified to the ODPC. This will be assessed on an individual basis according to the school's policy on Data Breach above, and where there is any doubt, legal advice will be sought.

5 Evaluation and Response

Following any serious Breach of Data incident, a thorough review will be undertaken by the response team and a report will be made to the Data Controller. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.

It will be reviewed every three years or more often should the Board of Management think it necessary in light of changed or amended legislation. Any review will continue to be guided by the school's characteristic spirit and commitment to its responsibilities under data protection legislation.