

**St. Corban's B.N.S.  
Fairgreen  
Naas  
Co. Kildare**



## **Data Protection/Record Retention Policy 2019**

### **St Corban's BNS 17254C**

#### **Introductory Statement**

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003. The policy applies to all school staff, the board of management, parents/guardians, pupils and others (including prospective or potential pupils and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

This policy was formulated by the staff and Board of Management of St Corban's BNS and applies to all staff and pupils as well as other partners with whom the school has business. It is the result of a policy review in 2008 on foot of a Data Protection Commissioner Inspection on Feb 22<sup>nd</sup> 2018.

The school recognises and accepts its responsibility as set out in the following:

- Data Protection Act 1998 and Data Protection (Amendment) Act 2003.
- Education Act 1998, section 9 (g), requiring a school to provide access to records to parents and to past pupils over 18.
- Education Act 1998, section 22.2 (b), requiring a school to regularly evaluate pupils and periodically report the results of the evaluation to the pupils and their parents.
- Education Welfare Act 2000, requiring a school to report school attendance and transfer of pupils.

St Corban's BNS (the school) as Data Controller will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information.

In particular, the school will comply with the Data Protection Principles as set out in the Data Protection Acts. These principles state that data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Used and disclosed only in ways compatible with these purposes
- Adequate, relevant and not excessive.
- Accurate and, where necessary, kept up to date.
- Kept no longer than necessary.
- Processed in accordance with data subject's rights.
- Kept in a safe and secure

The data controller must give a copy of his/her personal data to an individual on request.

## **Data Protection Principles**

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

- **Obtain and process *Personal Data* fairly:** Information on pupils is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of pupils etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.
- **Keep it only for one or more specified and explicit lawful purposes:** The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.
- **Process it only in ways compatible with the purposes for which it was given initially:** Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.
- **Keep *Personal Data* safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.
- **Keep *Personal Data* accurate, complete and up-to-date:** Pupils, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.
- **Ensure that it is adequate, relevant and not excessive:** Only the necessary amount of information required to provide an adequate service will be gathered and stored.
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given:** As a general rule, the information will be kept for the duration

of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

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

### Scope

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

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

### Definition of Data Terms

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

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

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

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

The Data Controller for the purpose of this policy is the Board of Management, St Corban's BNS.

### **Rationale**

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

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

### **Other Legal Obligations**

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

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a pupil who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the pupil in their education
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all pupils 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 pupil is transferring
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of pupils registered at the school on each school day
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers (SENOs) such information as the Council may from time to time reasonably request
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be “personal data” as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

### **Relationship to the Characteristic spirit of the school**

St Corbans BNS respects the rights of privacy of all those in the whole school community. St Corban’s BNS seeks to:

- enable each pupil 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 pupils, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals’ rights to privacy and rights under the Data Protection Acts.

### **Personal Data**

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

#### **A. Staff records:**

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

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Record of attendance

- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

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

- the management and administration of school business (now and in the future)
- to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- to facilitate pension payments in the future
- human resources management
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- and for compliance with legislation relevant to the school.

(c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Sensitive information is kept securely in locked rooms. (Principal's Office, Main Office, File Room)

(d) **Security:** Some data are kept in hardcopy in appropriate files in locked filing cabinets in locked rooms (Principal's Office, Main Office, Support Room 1, File Room). Some data are kept in digital form on school computers that are password protected.

## **B. Pupil records:**

(a) **Categories of pupil data:** These may include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the pupil'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)
  - religion
  - racial or ethnic origin
  - nationality
  - membership of the Traveller community, where relevant
  - whether English is the pupil's first language and/or whether the pupil 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 pupils (including at school 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 School reports
- Records of significant achievements
- Whether the pupil is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the pupil is engaged in work experience organised with or through the school/ETB 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 pupil to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes:** The purposes for keeping pupil records are:

- to enable each pupil to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible pupils can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child’s educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the pupil
- photographs and recorded images of pupils are taken to celebrate school achievements and pupil’s work, compile yearbooks and newsletters, update the school website, record school events, and to keep a record of the history of the school.
- to ensure that the pupil meets the school’s admission criteria
- to ensure that pupils meet the minimum age requirements for their course,
- to ensure that any pupil seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the pupil 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 pupil(or their parents/guardians in the case of a pupil under 18 years) documentation/information/ references to second-level educational institutions

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

kept securely in locked rooms (Principal's Office, Main Office, Support Room 1, File Room) Some data are kept on Aladdin and/or POD.

- (d) **Security:** Some data are kept in hardcopy in appropriate files in locked filing cabinets in locked rooms (Principal's Office, Main Office, Support Room 1, File Room). Some data are kept in digital form on school computers that are password protected or on secure digital platforms such as Aladdin or POD.

**C. Board of Management records:**

- (a) **Categories of Board of Management data:** These may include:
- Name, address and contact details of each member of the board of management (including former members of the board of management)
  - Records in relation to appointments to the Board
  - Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals, groups and organisations.
  - Financial reports and records
  - Child Protection Reports
  - Other specific projects/reports
- (b) **Purposes:** To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.
- (c) **Location:** In a secure, locked filing cabinet in the Principal's office and that only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Some data are kept in hardcopy in appropriate files in locked filing cabinets in the Principal's Office. Some data are kept in digital form on school computers that are password protected.

**D. Other records:**

*[School to insert other categories of data]*

*For example:*

The school 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):

**Creditors**

- (a) **Categories of data:** the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
  - address
  - contact details
  - PPS number
  - tax details
  - bank details and
  - amount paid.



- (b) **Purposes:** This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Some data are kept in hardcopy in appropriate files in locked filing cabinets in locked rooms (Principal's Office, Main Office, File Room). Some data are kept in digital form on school computers that are password and firewall protected.

### **Examination results**

- (a) **Categories:** The school will hold data comprising examination results in respect of its pupils. These include class, termly, annual, screening, diagnostic, continuous assessment and standardised test results.
- (b) **Purposes:** The main purpose for which these examination results and other records are held is to monitor a pupil's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Sensitive information is kept securely in locked rooms (Principal's Office, Main Office, Support Room 1, File Room) Some data are kept on Aladdin and/or POD.
- (d) **Security:** Some data are kept in hardcopy in appropriate files in locked filing cabinets in locked rooms (Principal's Office, Main Office, Support Room 1, File Room). Some data are kept in digital form on school computers that are password protected or on secure digital platforms such as Aladdin or POD.

### **Links to other policies and to curriculum delivery**

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

The following policies may be among those considered:

- Child Safeguarding Statement
- Anti-Bullying Policy
- Code of Behaviour
- Health & Safety Policy
- Mobile Phone Policy
- Admissions/Enrolment Policy

- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE etc.
- Enrolment Forms

### **Processing in line with data subject's rights**

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

Data subjects have a right to:

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

### **Dealing with a Data Access Request**

#### ***Section 3 access request***

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 30 days, where possible.

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

#### ***Section 4 access request***

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

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

Request must be responded to within 30 days, where possible

Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

### **Providing information over the phone**

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

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

### **Disclosure of records**

Elements of the data listed above may be disclosed, where relevant and appropriate, with the consent of the data controller to the following:

- Parents/guardians of pupils under 18 yrs
- Past pupils over 18yrs.
- School staff
- Outside agencies such as the DES, HSE (such as NCSE, etc)
- Schools to which pupils are transferring

Parental authorisation will be sought in advance of release of data to outside agencies. Parents may be given the information to pass on themselves. When a pupil transfers to another Primary School the new school will notify the original school and the original school will transfer records of attendance and educational progress to them with Parental permission. A standard School Report Form is used for this purpose. It may be given to the parents to pass on to the new school.

Outside agencies requesting disclosure of data must do so in writing. Parents/Guardians must also make such a request in writing to the Data Controller.

### **Responding to Requests**

The data controller will respond to requests within 30 days of receipt of same, where possible.

### **Guidelines on Retention time for Data**

All data will be retained for the duration of a pupil's enrolment/staff employment and for an additional period of between 1 and 8 years. In certain circumstances some data may be retained indefinitely. See Appendix 1 on Retention Schedule.

### **Personal Data and Pupil records**

The following will be kept for the duration of the child's enrolment in the school and the appropriate time thereafter (See Appendix 1 Retention Schedule)

- Parent/teacher meeting record cards
- End of year report from each year in school
- Standardised test results from each year in school
- Copy of most recent professional reports from outside agencies
- Copies of Individual Education Plans

Records held by the Principal in relation to child protection/child welfare will be held indefinitely.

### **Retention time for Administrative Data**

The procedures and schedule for retention of data is set out in Appendix 1 Retention Schedule.

Irrespective of the retention times set out in this policy, where any record is required in respect of existing legal proceedings, it will be held until the proceedings are concluded and the time allowed for appeal has passed.

### **Retention time for Board of Management Data**

The minute book of the Board of Management meetings will be held indefinitely.

### **Storage**

Data that is to be stored for eight or more years will be stored in a secure location in the locked File Room and will be accessible by designated personnel only. Old roll books and registers are stored in the Strong-room. Staff files are stored in the Principal's office.

Each Pupil's Main File is stored in the Main Office. Each Pupil's Classroom File is stored in each classroom in a locked Filing Cabinet. Each Pupil's Special Education Files is stored in Support Room 1 which is locked and only accessible to designated staff. When each pupil reaches the end of 6<sup>th</sup> class all of his pupil files are combined into his Main File and stored in the File Room for the appropriate duration. Data stored on computers is password and firewall protected. Data is stored for the period set out in the Records Retention Schedule which accompanies this policy.

### **Teacher Laptops**

Each teacher has the use of a school laptop which may contain data relating to pupils in his/her caseload/class. Teachers are responsible for maintaining and managing this data securely. All laptops are password and firewall protected.

### **Primary Online Database**

The Department of Education and Skills, which provides for the education and training of people resident in the State requires certain personal data on all learners to fulfil its function. Data is collected for all pupils enrolled in a recognised school aided by the DES. This data is stored on the Primary Online Database. All of the data is provided by the school the pupil attends. Where a pupil moves school both the original school and the new school update POD with the relevant information. Certain data are considered sensitive personal information and in order to collect and process this information the explicit written consent of the pupil's parents or guardian is required. This data is Religion and Ethnic or Cultural Background. This is sought during the Enrolment Process. Where consent has been granted you are free to withdraw that consent at any time by contacting the POD Helpline on (01) 8892311 or [pod@education.ie](mailto:pod@education.ie)

For more information on POD see Appendix ????

### **Aladdin**

St Corban's uses Aladdin Schools as an Administration Management System. It is an online Management Information System/ Pupil Information System specifically designed to simplify administration in primary schools. It is used as an information hub, for communication, for recording the roll electronically and recording attendance, for recording money paid, for assessment and reporting, for planning, for text messaging and for policy dissemination. Pupil information is stored on the system. It uses Google to store our school information in data centres within the EU that are independently audited and certified to international standards. Aladdin has superior data security with extended SSL encryption and this means that even if Aladdin is accessed across an unsecured wireless connection the data is fully protected. Aladdin eliminates the chance of physical loss and theft of our data and this, along with our other certified security measures, enhances our school's compliance with data protection law. We use Aladdin as a Roll Book, a means of in-school communication and for storing information on pupils. Each teacher has his/her own log-in details and password and only has access to his/her class or caseload.

### **Notification of a Breach – each Staff Member's Duty to Notify**

As soon as a member of St Corban's staff becomes aware that personal data has been compromised (e.g. through loss of a portable device, misaddressing of labels, sensitive information left where unauthorised viewing could take place, etc), the staff member shall immediately notify the Principal and complete the **Data Security Breach Incident Report (See Appendix )**.

The Principal who receives the notification will investigate the issues surrounding the breach. The seriousness of the breach will determine the type of investigation that will take place. It may include an on-site examination of systems and procedures. In the event of a serious data security breach the Principal will escalate the matter and the Board of Management will be informed and contact will be made with the Office of the Data Protection Commissioner for advice and clarification. The advice of the Data Commissioner will guide the process.

Where appropriate or advised the Principal will put a communication plan in place to contact the owner of the data involved (the data subject). Security of the medium used for notifying individuals of a breach of data protection procedures and urgency of situation should be borne in mind. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the school is willing to do to assist them.

#### **Protocol for action in the event of breach**

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the school will follow the following protocol.

The school will seek to contain the matter and mitigate any further exposure of the personal data held. The school shall have regard to the "Incident Response DOs and DON'Ts for IT systems" advice set out in the Appendix. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011.

#### **Reporting of incidents to the Office of Data Protection Commissioner:**

All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 72 hours thereafter). The school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see contact details below).

Data Protection Commissioner  
Office of the Data Protection Commissioner  
Canal House, Station Road, Portarlinton, Co. Laois  
**Tel:** 1890 252 231  
**Email:** [info@dataprotection.ie](mailto:info@dataprotection.ie)  
**Website:** [www.dataprotection.ie](http://www.dataprotection.ie)

### **Implementation arrangements, roles and responsibilities**

In our school the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities. The school staff, under the direction of the Principal will implement and monitor this policy. The Principal and the Board of Management will ensure records are maintained and stored appropriately.

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

<b>Name</b>	<b>Responsibility</b>
Board of Management:	Data Controller
Principal:	Implementation of Policy
School staff:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

### **Ratification and Communication**

When the Data Protection Policy has been ratified by the board of management, it becomes the school's agreed Data Protection Policy. It is shared with all staff.

Parents/guardians and pupils are informed of the Data Protection Policy from the time of enrolment of the pupil.

### **Implementation Date**

This new policy is effective following ratification by the Board of Management.

### **Timetable for Review**

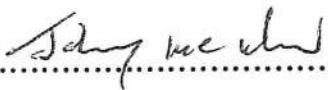
The operation of the new procedures be reviewed/ amended when required.

### **Communication**

A copy of this policy has been shared with each teacher. It is available on the school website and is available for parents to view in the school.

### **Ratification**

This policy was ratified by the Board of Management in 2019.

Signed: .....  ..... Date: 15/1/19 .....

**Chairperson of the Board of Management**

*(For and on behalf of the Board of Management)*

Appendix 1

**Data Security Breach – Incident Report**

**Breach ID:**

**When did the breach take place?**

**When was the breach discovered?**

**Who reported the breach?**

**Were there any witnesses? If Yes, state Names.**

**Please provide details of the breach:**

**Were any IT systems involved? If so please list them.**

Is any additional material available e.g. error messages, screen shots, log files,

Any additional comments?

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

Time: \_\_\_\_\_

**For Breach Management Team Use**

Details logged by \_\_\_\_\_

Severity of the breach (0 being minor, 5 being critical)

0            1            2            3            4            5

Data Subjects to be notified      Yes         No  

Details: \_\_\_\_\_

\_\_\_\_\_

Data Protection Commissioner to be notified      Yes         No  

Details (Date/time, note of advice received): \_\_\_\_\_

\_\_\_\_\_

Gardaí to be notified      Yes         No  

Details: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



## Appendix 2

# Guidelines for Staff

**Under the GDPR a breach which is reportable to the Data Protection Commission must be reported not later than 72 hours after having become aware of it. All breaches or suspected breaches should therefore be reported to the Principal without delay for assessment.**

A personal data protection breach ("data breach" in short) usually occurs when:

- there is an unauthorised or accidental **disclosure** of, or access to, personal data.
- there is an unauthorised or accidental **alteration** of personal data.
- there is an accidental or unauthorised **loss of access to, or destruction of,** personal data.

The GDPR defines a data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Data breaches may occur in a variety of contexts, such as:

- Loss or theft of data (e.g. on a memory stick, laptop or paper records)
- Inappropriate access controls (e.g. using unsecure passwords)
- Equipment failure
- Confidential information being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving documents on top of shared photocopiers)
- Disclosing confidential data to unauthorised individuals
- Human error (e.g. emails being sent to the wrong recipient)
- Hacking, viruses or other security attacks on IT equipment systems or networks e.g. Ransomware
- Breaches of physical security (e.g. forcing of doors/windows/filing cabinets)

If a data breach has occurred, you will be asked to complete the Data Protection Breach Report Template and give it to the Principal as soon as possible. It is much better to report a data protection breach straight away than to "cover it up" and risk negative consequences down the line. A data protection breach is not a disciplinary issue, and once the breach has been reported the Principal will handle things from there.

**This following is a summary guide to the most common data protection issues encountered by school staff.**

- If you have to share personal data in the course of performing school functions, make sure you only share the data with colleagues who need to know it.
- If a parent / guardian of a student contacts you to request their son or daughter's personal data (e.g. exam results, registration details) speak with the Principal. If a past pupil is over 18, you should not release that data unless you have the written consent of the past pupil to do so.
- If you are emailing more than one person at a time, you should always use the "Bcc" option to avoid sharing students' personal data (email address) with other students.

- If you are unsure as to whether a particular set of data should be retained or disposed of, refer to the Data Retention Schedule.
- If a data breach occurs, you should immediately contact the Principal for further details.

### **Appendix 3**

#### **Incident Response DOs and DON'Ts for IT systems**

##### ***DO'S***

- immediately isolate the affected system to prevent further intrusion, release of data, damage etc.
- use the telephone to communicate. Attacker may be capable of monitoring e-mail traffic
- preserve all pertinent logs, e.g. firewall, router and intrusion detection system.
- make back-up copies of damaged or altered files and keep these backups in a secure location.
- identify where the affected system resides within the network
- identify all systems and agencies that connect to the affected system
- identify the programs and processes that operate on the affected system(s), the impact of the disruption and the maximum allowable outage time.
- in the event the affected system is collected as evidence, make arrangements to provide for the continuity of services i.e. prepare redundant system and obtain data back-ups.

##### ***DON'Ts***

- delete, move or alter files on the affected systems
- contact the suspected perpetrator
- conduct a forensic analysis

### **Appendix 4 Aladdin**

### **Appendix 5 POD**

### **Appendix 6 Records Retention Schedule**

## NOTES

### **Sort out Appendices:**

POD Sheet for Appendix  
Aladdin Sheets for Appendix  
Records Retention Schedule

Put in a section on Digitally stored documents (Aladdin and POD) in the  
Records Retention Schedule

