Scoil Thomais, Laurel Lodge, Castleknock, Dublin 15

Data Protection Policy – March 2016

Introductory Statement

Scoil Thomáis 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, 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. 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***.**

Purpose of the Policy:

The Data Protection Acts 1988 and 2003 apply to the maintenance 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 and to explain those obligations to school staff. The policy also informs staff, pupils, parents /guardians as to how their data will be treated.

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 are summarised as follows:

- **Obtain and process *Personal Data* fairly**:
- **Keep it only for one or more specified and explicit lawful purposes**:
- **Process it only in ways compatible with the purposes for which it was given initially**:
- **Keep *Personal Data* safe and secure**
- **Keep Personal Data accurate, complete and up-to-date**:
- **Ensure that it is adequate, relevant and not excessive**:
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**:
- **Provide a copy of their *personal data* to any individual, on request**

Definition of Data Protection Terms

Data means information in a form that can be processed, both *automated data* (e.g. electronic data) and *manual data*.
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, 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 Principal on behalf of the Board of Management. The Principal ensures the application of the Data Protection Act within the school. All staff have responsibility to protect the security and integrity of all school data accessible to them and must co-operate with data protection guidelines.

Rationale for Data Protection Policy

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

The school acknowledges its responsibilities under data protection law and seeks to put in place safe practices to safeguard individual's personal data. 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.

Relationship to characteristic spirit of Scoil Thomáis

The terms of this policy support the school mission statement which states that Scoil Thomáis promotes the fullest possible development of each child socially, emotionally, spiritually, physically and intellectually so that he/she
• May lead a full enjoyable life as a child. • Be prepared to avail of further education. • Be able to contribute to society as an adult and enjoy leisure time.

Other Legal Obligations

Implementation of this policy takes into account the school's other legal obligations and responsibilities.
Those directly relevant to data protection include:

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, Túsla 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).

<u>The Data Under The Control Of The School Can Be Categorised As Follows:</u>

1. Pupil Data (Personal Data & Pupil Records) – *this list is may be expanded as necessary*

Pupil Data **includes** information which is sought and recorded at enrolment and information which is obtained during the course of a pupil's enrolment in the school. These records may include (this list is not exhaustive) :
name, address and contact details, PPSN, date and place of birth, name & addresses of parents/guardians & contact details (including any special arrangements with regard to guardianship, custody or access), religious belief, racial or ethnic origin, Language spoken, any relevant 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, School Attendance and punctuality records, Photographs and recorded images of students, Academic record – subjects studied, class assignments, examination results as recorded on school reports, Records of significant achievements, exemptions from Irish (where relevant), Records of behavioural issues/investigations and/or sanctions imposed, Other records e.g. records of any serious injuries/accidents etc. Psychological/Clinical/Occupational Therapy/Speech and Language Assessments , Standardised Test Results , Screening Tests, Teacher – designed tests, Diagnostic Tests Reports, Individual Education Plans (IEP) and Individual Profile and Learning Programmes (IPLP), Learning Support/SEN Data such as referrals for learning support/records of permission etc, Portfolios of pupils work etc , Records of any reports the school may 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 DES Child Protection Procedures) and any other relevant data as deemed necessary by the school data controller.

Location: Pupil data is maintained in electronic form on the 'Aladdin' Pupils Management System and relevant hard copy formats are retained in the Principal/Deputy Principal's office, Secretary's office and in Class/SEN teacher's classroom.
Security: Hard copies of records are retained in a locked filing cabinet accessible only by authorised school staff.
Pupil Attendance records (currently in Leabhair Rolla), PPSN and other sensitive and non-sensitive data are also on the Pupil Online Data (POD) system (Department of Education and Skills) since 2015 and are maintained in line with DES Guidelines. Access to pupil records is restricted to authorised personnel. School Staff are required to maintain the confidentiality and security of any data to which they have access.

2. Staff Data (Personal Data & Staff Records) - ***this list is may be expanded as necessary***
This data relates to personal and professional details of school staff such as, Name, date of birth, address and contact details, PPS/payroll number**,** Records of application, appointment and contractual arrangements to the school and appointment and contractual arrangements to POR posts**,** Details of statutory and non-statutory leave ie sick leave, career breaks etc. Details of work record (qualifications, professional development, classes taught, 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) and any other relevant data as deemed necessary by the school data controller.

Location: Staff records are retained in a secure, locked filing cabinet accessible only by authorised school staff. School staff are required to maintain the confidentiality of any data to which they have access.
Security: The records of staff members current and former are kept in manual and digital format in personal files and in digital format as on OnLine Claims System - OLCS provided by Dept of Education and Skills. Manual staff record files are retained in the Principals/Deputy Principals Office. Access to staff records is restricted to authorised personnel.

3. **Board of Management Records -** ***this list is may be expanded as necessary***
Data retained under BOM records include: name, address and contact details member sof 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 relevant past and current correspondence to the Board which may include references to particular individuals etc , school financial accounts and records, contracts etc and any other relevant data as deemed necessary by the school data controller.

Location: BOM records are retained in the Principals Office in both open filing and locked filing cabinets and on school computer system protected by passwords. Access to BOM records is restricted to authorised personnel. School Staff are required to maintain the confidentiality of any data to which they have access.

4.Other Records - ***this list is may be expanded as necessary***
Records relating to contacts with outside agencies such as CPSMA/insurance companies/legal advice/ buildings and lands etc. will be securely maintained in the manner appropriate to its origins e.g paper correspondence or email as appropriate. The school will hold other records relating to communication with individuals and agencies relevant to the operation of the school ie Tusla etc. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database) as appropriate.

5.**CCTV Images/Recordings**
A CCTV system for security purposes is installed at the front door, at the main reception entrance area and at three other external areas of the school. The CCTV system records images of staff, pupils and members of the public who are on the school premises on a 24/7 basis. There is signage to this effect at various points on the school premises.

Location: Cameras are located externally as detailed above. Recording equipment is located in the School
Security: Access to images/recordings is restricted to the Chairperson BOM, Principal/ Deputy Principal and School Secretary. Hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

NOTE - DES RECOMMENDATIONS REGARDING SAFE STORAGE AND RETENTION PERIODS FOR IMPORTANT RECORDS

Responsibilities of School Staff: School staff must adhere to data protection guidelines in relation to obtaining, storing and accessing all school data as covered by this policy. This includes data in manual and electronic form and data held on web based school administration systems. It is acknowledged that it may be necessary for school staff to access school based data remotely in the course of their professional work (ie when compiling online end of year school reports). Staff are reminded that they must always take all necessary precautions to safeguard the security and privacy of school data at all times – both in school and outside of school. This responsibility is especially relevant for staff when accessing electronic or web based school data outside of school. Personal data on pupils and sensitive school data school should not be stored by school staff on personal computers or other electronic devices. In cases where there is an unintentional breach of data (email or hard copy) the staff member/s involved should follow school protocol on the matter as outlined in Appendix 1 of this policy. **SCHOOL PROCEDURES IN THE CASES OF DATA BREACH**

Processing Data

Scoil Thomáis will process data in accordance with the rights of the data subjects' ie pupils, parents/guardians, school staff and BoM members and all others whose records are covered by this policy. *Data subjects have a right to:*
(a) Request access to any data held about them by a data controller; (b) Prevent the processing of their data for direct-marketing purposes; (c) Ask to have inaccurate data amended; (d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with a Data Access Requests

Section 3 Access Request: Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days. The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 Access Request: Under Section 4 of the Data protection Acts 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). The following conditions apply:

- The Data Access request (S.4) will be responded to within 40 days and a fee of €6.35 will apply in Scoil Thomais.
- 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 data controller to comply with the request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on case-by-case basis.
- No personal data will 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.

Implementation of the Policy - Roles and Responsibilities

The School Principal on behalf of the BoM is the data controller, and co-ordinates the implementation of the Data Protection Policy. The Principal assisted by the Deputy Principal have responsibility to ensure that all school 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
Principal on behalf of BOM	Data Controller
Principal/Deputy Principal and all staff	Implementation of Policy
Teaching and Non Teaching Staff	Awareness of responsibilities + adhere to the policy
Office Staff	Security, confidentiality + adhere to the policy
IT Contractors	Security, encryption, confidentiality

Review of the Policy: This policy will be reviewed and if necessary amended, by the Board of Management.

Ratification of Policy: This policy has been drawn up in consultation with Scoil Thomáis staff, parents and BOM and was ***ratified by Scoil Thomáis Board of Management on 8th March 2016***

APPENDIX 1 : Procedures in the event of a data breach such as an email being sent unintentionally or a hard copy document mailed unintentionally,

1. When addressing any email ensure you have used the correct addresses for the intended recipients.
   [With automatic address selection in Outlook it is possible to send a mail to an unintended recipient by mistake.]
2. When sending hard copy documents by mail ensure you have used the correct addresses for the intended recipients.
3. Before sealing the envelope or hitting the send button *stop* and *check* where it is going and what is enclosed.
   The following guidelines will assist in the event that a hard copy document is mailed or an email is sent to an unintended recipient.

Unintentional Email Being Sent !
Immediately: Attempt to recall the email**.** If unsuccessful: Call the unintended recipient and explain that the mail was sent by mistake due to an unintended human error despite internal policies and requirements as regards confidential material and establish the following:

- Was the Email opened by them or by anyone else who had access to their email? If so, at what time was it opened?
- If not opened ask that they not open or read the mail, and that they not circulate the mail, and that they delete the mail permanently in such a way that it cannot be retrieved and shared in the future
- Was the Email circulated by them or by anyone else? If so, to whom and when? If not circulated ask them not to do so
- Was the Email read by them or by anyone else who had access to their email? If so, at what time did this occur, was the Email or any of its contents shared either verbally or in writing with any other persons? If not ask that they not read the mail, and that they not circulate the mail, and that they delete the mail permanently in such a way that it cannot be retrieved and shared in the future
- Ask that they confirm that neither the Email itself nor any of its contents will, at any stage in the future, be shared (either verbally or in writing) by them, or by any other person within their organisation, with any other person either within or outside their organisation.
- Ask that they confirm with you when the Email has been deleted and when this occurred.
- Establish their role in their organization if not already known

If you are unable to speak to the person directly, leave a voice message regarding the above. Send an email (without repeating any of the contents of the unintended mail or including same in a chain) to the person that states the prior mail was sent by mistake due to an unintended human error and ask that they not open, read or circulate the mail but delete same immediately and that they kindly confirm when they have done this.
Make follow up calls until you have confirmation that the mail has been deleted.

1. Document the above actions and when they occurred.
2. Inform the Data Controller [Principal].
3. The Data Controller [Principal] will need to consider whether any other external parties need to be advised of the event depending on who may be affected by the same and to action same as the circumstances require.
4. Do not discuss the matter with external parties without the agreement of the Data Controller[Principal]
5. The internal staff involved should consider whether any further action is required in the circumstances and if any steps can be taken to ensure this does not happen again and to action same as appropriate.
6. Create an Incident report that documents the above and send this to the Data Controller [Principal]

Hard copy documents are mailed in error !
Immediately: Call the unintended recipient and tell them the mail was sent by mistake due to an unintended human error despite internal policies and requirements as regards confidential material and establish the following:

- Was the mail opened by them or by anyone else who had access to their email? If so, at what time was it opened
- If not opened ask that they not open or read the mail, and that they not circulate the mail, and that they return the mail
- Was the mail circulated by them or by anyone else? If so, to whom and when? If not circulated ask them not to do so
- Was the mail read by them or by anyone else who had access to their mail? If so, at what time did this occur, was the mail or any of its contents shared either verbally or in writing with any other persons? If not ask that they not read the mail, and that they not circulate the mail, and that they return the mail
- Ask that they confirm that neither the mail itself nor any of its contents will, at any stage in the future, be shared (either verbally or in writing) by them, or by any other person within their organisation, with any other person either within or outside their organisation.
- Ask that they confirm with you when the mail has been returned and when this occurred.
- Establish their role in their organization if not already known

If you are unable to speak to the person directly, leave a voice message regarding the above.
Send an email (without repeating any of the contents of the unintended mail or including same in a chain) to the person that states the hard copy mail was sent by mistake due to an unintended human error and ask that they not open, read or circulate the mail but return same immediately and that they kindly confirm when they have done this. Make follow up calls until you have confirmation that the mail has been returned.

1. Document the above actions and when they occurred.
2. Inform the Data Controller [Principal].
3. The Data Controller [Principal] will need to consider whether any other external parties need to be advised of the event depending on who may be affected by the same and to action same as the circumstances require.
4. Do not discuss the matter with external parties without the agreement of the Data Controller[Principal]
5. The internal staff involved should consider whether any further action is required in the circumstances and if any steps can be taken to ensure this does not happen again and to action same as appropriate.
6. Create an Incident report that documents the above and send this to the Data Controller [Principal]