SCOIL URSULA SLIGO

Data Protection Policy (GDPR)

Scoil Ursula

Data Protection Policy (GDPR)

Title

Data Protection Policy of Scoil Ursula Sligo

Introductory Statement

This policy has been formulated in consultation with the staff, parents and Board of Management in December 2018 in order to comply with the EU General Data Protection Regulation (GDPR).

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 to 2018 and the EU General Data Personal Regulation (GDPR).

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the 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.

Scoil Ursula operates a "***Privacy by Design***" method in relation to Data Protection. This means we plan carefully when gathering personal data so that we build in the ***data protection principles*** as integral elements of all data operations in advance. We audit the personal data we hold in order to:

1. be able to provide access to individuals to their data;
2. ensure it is held securely;
3. document our data protection procedures;
4. enhance accountability and transparency.

Data Protection Principles

The school is a *data controller* of *personal data* relating to its past, present and future staff, students, 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 to 2018 and GDPR, which can be summarised as follows:

1. **Obtain and process *Personal Data* fairly**:

Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals

applying for positions within the School, parents/guardians of students 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 Legislation and the terms of this Data Protection Policy. The information will be obtained and processed fairly. (See: Appendix 1)

2. Consent:

Where consent is the basis for provision of personal data, (e.g. data required to join sports teams/ after-school activity or any other optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Scoil Ursula will require a clear affirmative action e.g. ticking of a box/signing a document/ proceeding with an online application to indicate consent. Consent can be withdrawn by data subjects in these situations. (See: Appendix 2)

3. 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.

4. 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.

5. 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.

6. Keep Personal Data accurate, complete and up-to-date:

Students, 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.

7. **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.

8. **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 (See: School Record Retention Table – Appendix 3)

9. **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 (See: Appendix 4)

Scope

Purpose of the Policy: The Data Protection Legislation applies 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, students and their parents/guardians how their data will be treated.

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

Definition of Data Protection 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 form part of a relevant filing system.

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

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

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

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the board of management, Scoil Ursula.

Data Subject – is an individual who is the subject of personal data.

Data Processing – performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data;
- Collecting, organising, storing, altering or adapting the data;
- Retrieving, consulting or using the data;
- Disclosing the data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the data;

Data Processor – a person who processes personal information on behalf of a data controller, but **does not include an employee of a data controller** who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data (e.g. Aladdin; school accounting / wages processors)

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means any compromise or loss of personal data, no matter how or where it occurs

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 to 2018 and the GDPR.

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 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, Tusla, 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, mandated persons in schools 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 characteristic spirit of the School

Scoil Ursula seeks to

- enable each student to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The 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, sick leave certs 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
- 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.

(d) **Security:** Records are kept in manual form (personal file within a *relevant filing system*) and/or on computer record (database or on cloud-based administration software within our Aladdin System. Manual data is kept in locked filing cabinets only accessible to those personnel with whom it is applicable. Computer or cloud based data is stored on the Principal's and/or the Secretary's computer and on the Aladdin administrative system also only accessible to relevant personnel. In the

case of the Aladdin system, the company provide encrypted security to protect all stored data.

B. <u>Student records:</u>

(a) **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
- Photographs and recorded images of students (including at school events and noting achievements).
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the 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).

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

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the student

- photographs and recorded images of students are taken to celebrate school achievements, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's Admissions Policy and Enrolment Form.
- 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 Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers

(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:** Records are kept in manual form (personal file within a *relevant filing system*) and/or on computer record (database or on cloud-based administration software within our Aladdin System. Manual data is kept in locked filing cabinets only accessible to those personnel with whom it is applicable. Computer or cloud based data is stored on the Principal's and/or the Secretary's computer and on the Aladdin administrative system also only accessible to relevant personnel. In the case of the Aladdin system, the company provide encrypted security to protect all stored data.

C. <u>Board of management records:</u>

(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.

(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 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:** Records are kept in manual form (personal file within a *relevant filing system*) and/or on computer record (database or on cloud-based administration software within our Aladdin System. Manual data is kept in locked filing cabinets only accessible to those personnel with whom it is applicable. Computer or cloud based data is stored on the Principal's and/or the Secretary's computer and on the Aladdin administrative system also only accessible to

relevant personnel. In the case of the Aladdin system, the company provide encrypted security to protect all stored data.

D. Other records:

The school may 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):

- Student Teachers on Teaching Practice or Observation
- Other Students on Placements
- Substitute Teachers on the Scoil Ursula Sub List
- Coaches and officials from various sporting organisations and agencies with whom Scoil Ursula collaborates with.
- Personnel from various agencies and organisations with whom the school has dealings with e.g. TUSLA, HSE, NCSE, SESS, NEPS, DES etc.

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:** Records are kept in manual form (personal file within a *relevant filing system*) and/or on computer record (database or on cloud-based administration software within our IBB Banking System. Manual data is kept in locked filing cabinets only accessible to those personnel with whom it is applicable. IBB data is password protected and only accessible to the Chairperson, Principal, Secretary and Treasurer via an AIB Digipass which is encrypted for security purposes.

Charity tax-back forms

(a) **Categories of data**: the school may hold the following data in relation to donors who have made charitable donations to the school:
- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

(b) **Purposes**: Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit 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:** Records are kept in manual form (personal file within a *relevant filing system*) and/or on computer record (database or on cloud-based administration software within our Aladdin System. Manual data is kept in locked filing cabinets only accessible to those personnel with whom it is applicable. Computer or cloud based data is stored on the Principal's and/or the Secretary's computer and on the Aladdin administrative system also only accessible to relevant personnel. In the case of the Aladdin system, the company provide encrypted security to protect all stored data.

Test results

(a) **Categories**: The school will hold data comprising test results in respect of its students. These include class, screening, diagnostic and standardised results.

(b) **Purposes**: The main purpose for which these results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about levels of progress. The data may also be aggregated for statistical/reporting purposes, such as School Self Evaluation and annual reporting to parents. 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.

(c) **Security:** Records are kept in manual form (personal file within a *relevant filing system*) and/or on computer record (database or on cloud-based administration software within our Aladdin System. Manual data is kept in locked filing cabinets only accessible to those personnel with whom it is applicable.

Computer or cloud based data is stored on the Principal's and/or the Secretary's computer and on the Aladdin administrative system also only accessible to relevant personnel. In the case of the Aladdin system, the company provide encrypted security to protect all stored data.

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 Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Mobile Phone Code
- Admissions/Enrolment Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE etc.

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) Know what personal data the school is keeping on them
(b) Request access to any data held about them by a data controller
(c) Prevent the processing of their data for direct-marketing purposes
(d) Ask to have inaccurate data amended
(e) Ask to have data erased once it is no longer necessary or irrelevant (See: Appendix 5)
(f) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Personal Data Breaches

All incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 72 hours.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the BoM must communicate the personal data breach to the data subject without undue delay.

If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (BoM) without undue delay.

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 (See: Appendix 4) 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

Individuals are entitled to a copy of their personal data on written request (See: Appendix 4).

- 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 40 days
- Fee may apply but cannot exceed €6.35
- 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.

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 following personnel have responsibility for implementing the Data Protection Policy:

Name	**Responsibility**
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Monitoring the implementation of the policy

The implementation of the policy is monitored by the principal and the board of management.

Reviewing and evaluating the policy

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

Ratification & communication

The Board of Management ratified this policy on the _____ of

_____, _____

Signed: _____, (Chairperson, BOM)

Scoil Ursula does not have adequate resources to disseminate all of its policies to all the concerned members of the wider school community. The policy is communicated to the members of the BOM and is available to the wider school community through the parents' representatives on the BOM. All Scoil Ursula policies are available for inspection in the school and on www.scoilursula.com

Appendix 1

Fair Processing

Fair Processing of personal data

Section 2A of the Acts details a number of conditions, at least one of which must be met, in order to demonstrate that personal data is being processed fairly. These conditions include that the data subject has consented to the processing, or that the processing is necessary for at least one of the following reasons:

1. The performance of a contract to which the data subject is party, or
2. In order to take steps at the request of the data subject prior to entering into a contract, or
3. In order to comply with a legal obligation (other than that imposed by contract), or
4. To prevent injury or other damage to the health of the data subject, or
5. To prevent serious loss or damage to the property of the data subject, or
6. To protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged, or
7. For the administration of justice, or
8. For the performance of a function conferred on by or under an enactment or,
9. For the performance of a function of the Government or a Minister of the Government, or
10. For the performance of any other function of a public nature performed in the public interest by a person, or
11. For the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject

Fair processing of sensitive personal data

If processing sensitive data, you must satisfy the requirements for processing personal data set out above along with at least one of the following conditions (set out in section 2B of the Acts):

1. The data subject has given explicit consent, or
2. The processing is necessary in order to exercise or perform a right or obligation which is conferred or imposed by law on the data controller in connection with employment, or
3. The processing is necessary to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent, or
4. The processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld, or
5. The processing is carried out by a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation, or
6. The information being processed has been made public as a result of steps deliberately taken by the data subject, or

7. The processing is necessary for the administration of justice, or
8. The processing is necessary for the performance of a function conferred on a person by or under an enactment, or
9. The processing is necessary for the performance of a function of the Government or a Minister of the Government, or
10. The processing is necessary for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights, or
11. The processing is necessary for medical purposes, or
12. The processing is necessary in order to obtain information for use, subject to, and in accordance with, the Statistics Act, 1993, or
13. The processing is necessary for the purpose of assessment of or payment of a tax liability, or
14. The processing is necessary in relation to the administration of a Social Welfare scheme

Appendix 2

Consent

Where consent is the basis for provision of personal data (e.g. data required to join sports team/ after-school activity/or optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Each school will require a clear, affirmative action e.g. ticking of a box/signing a document, to indicate consent. Consent can be withdrawn by data subjects in these situations

To ensure that the school's practices are open and transparent and to obtain data fairly the data subject must, at the time the personal data is being collected, be made aware of:

1. the name of the data controller (i.e. School BoM)
2. the purpose/rationale for collecting the data and any secondary uses of their personal data which might not be obvious to them
3. the persons or categories of persons to whom the data may be disclosed e.g. DES
4. other third parties operating in the education and welfare sphere eg. NCSE, TUSLA, NEPS, SESS, the HSE,TUSLA, An Garda Síochána
5. other third parties with whom the School contracts, such as cloud-based school administration software companies, accountants, insurance companies, lawyers, etc.
6. whether replies to questions asked are obligatory and the consequences of not providing replies to those questions
7. the existence of the right to access their personal data
8. the right to rectify their data if inaccurate or processed unfairly
9. any other information which is relevant so that processing may be fair and to ensure that the data subject has all the information that is necessary to facilitate their awareness of how their data will be processed

Where you use application forms or standard documentation in school for enrolment or other purposes, you should explain your purposes/uses etc. clearly on such forms or documentation

No age limit is associated with consent. However, it is important that the data subject appreciates the nature and effect of such consent. Therefore, different ages might be set for different types of consent. Where a person is unlikely to be able to appreciate the nature or effect of consent, by reason of physical or mental incapacity or age, then a parent, grandparent, uncle, aunt, brother, sister or guardian may give consent on behalf of the data subject. These are the only circumstances in which a third party may give consent on behalf of a data subject

Fair Obtaining: Test Yourself

When people are giving you information, you should be able to answer YES to the following questions:-

1. do they know what information you will keep about them?
2. do they know the purpose for which you keep and use it?
3. do they know the people or bodies to whom you disclose or pass it?

In general, the fair obtaining principle requires that every individual about whom information is collected for holding will be aware of what is happening

Appendix 3

School Record Retention Table

Pupil Related	Retention Periods
School Register/Roll Books Enrolment Forms	Indefinitely Hold until pupil is 25 Years
Disciplinary notes	Never Destroy
Test Results – Standardised	Never Destroy
Psychological Assessments etc.	Never Destroy
SEN Files/IEPS	Never Destroy
Accident Reports	Never Destroy
Child Protection Reports/Records	Never Destroy
S.29 Appeals	Hold until pupil is 25 Years
Interview Records	
Interview Board Marking Scheme Board of Management notes (for unsuccessful candidates)	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
Staff Records	
Contract of Employment Teaching Council Registration Vetting Records	Retention for duration of employment + 7 years

Accident/Injury at work Reports	(6 years to make a claim against the school plus 1 year for proceedings to be served on school)
BoM Records	
BOM Agenda and Minutes	Indefinitely 28 days normally. In the event of criminal investigation – as long as is necessary
Payroll & Taxation	Revenue require a 6-year period after the end of the tax year
Invoices/receipts	Retain for 7 Years Indefinitely
Audited Accounts	Indefinitely

Why, in certain circumstances, does the Data Protection Commission recommend the holding of records until the former pupil has attained 25 years of age?

The reasoning is that a pupil reaches the age of majority at 18 years and that there should be a 6-year limitation period in which it would be possible to take a claim against a school, plus 1 year for proceedings to be served on a school. The Statute of Limitations imposes a limit on a right of action so that after a prescribed period any action can be time barred.

Data that becomes obsolete will be shredded. The school may employ the services of a private company in the destruction of such data.

Appendix 4

Personal Data Access Request Form

Request for a copy of Personal Data under the Data Protection Acts 1988 to 2018

<u>Important:</u> Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

Full Name:	
Maiden Name *(if name used during* your school duration*)*	
Address:	
Contact number *	Email addresses *

* We may need to contact you to discuss your access request

Please tick the box which applies to you:

Parent/ Guardian of current Pupil	**Former Pupil**	**Current Staff Member**	**Former Staff Member**
Name of Pupil:		Date of Birth of Pupil:	
Insert Year of leaving:		Insert Years From/To:	

Data Access Request:

I, …… [name] wish to make an Access Request for a copy of personal data that Scoil Ursula holds about me/my child. I am making this access request under Data Protection Acts 2013 to 2018

To help us to locate your personal data, please provide details below, which will assist us to meet your requirements e.g. description of the category of data you seek.

Any other information relevant to your access request (e.g. if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings as otherwise it may be very difficult or impossible for the school to locate the data)

This **Access Request** must be accompanied with a copy of photographic identification e.g., passport or drivers licence. I declare that all the details I have given in this form are true and complete to the best of my knowledge.

Signature of Applicant ……..

Date: …….

Please return this form to the relevant address:

The Chairperson Board of Management, Scoil Ursula, Strandhill Road, Sligo.

Appendix 5

Your rights as a data subject

1. Right to have your data processed in accordance with the Data Protection Acts - to have your personal information obtained and processed fairly, kept securely and not unlawfully disclosed to others

2. Right to be informed - to know the identity of the data controller and the purpose for obtaining your personal information

3. Right of access - to get a copy of your personal information

4. Right of rectification or erasure - to have your personal information corrected or deleted if inaccurate

5. Right to block certain uses - to prevent your personal information being used for certain purposes

6. Right to have your name removed from a direct marketing list - to stop unwanted mail

7. Right to object - to stop some specific uses of your personal information

8. Employment rights - not to be forced into accessing personal information for a prospective employer

9. Freedom from automated decision making - to have a human input in the making of important decisions relating to you

10. Rights under Data Protection and Privacy in Telecommunications Regulations - to prevent your phone directory entry details from being used for direct marketing purposes

Appendix 6

The 8 Rules of Data Protection

1. **Obtain and process information fairly**
2. **Keep it only for one or more specified, explicit and lawful purposes**
3. **Use and disclose it only in ways compatible with these purposes**
4. **Keep it safe and secure**
5. **Keep it accurate, complete and up-to-date**
6. **Ensure that it is adequate, relevant and not excessive**
7. **Retain it for no longer than is necessary for the purpose or purposes**
8. **Give a copy of his/her personal data to that individual on request**