



Policy on Data Protection

Introduction:

The [Canal Way](#) ETNS Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003. This policy was first developed in 2017 and was reviewed in May 2020. It will be reviewed periodically to incorporate any changes as to how [Canal Way](#) ETNS treats data that it collects and relevant legislative changes.

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, in so far 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.

Purpose

1. Data protection principles:

The school is a data controller of personal data relating to its 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:

1.1 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.

1.2 Keep it only for one or more specified and explicit lawful purposes:

Canal Way ETNS will inform individuals of the purpose of collecting 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.

1.3 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.

1.4 Keep personal data safe and secure:

Only those with necessary professional requirements 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 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.

1.5 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.

1.6 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.

1.7 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 pupil. 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.

1.8 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:

The Data Protection 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 in the school in so far as the school handles or processes their personal data in the course of their dealings with the school.

2. Policy statement:

2. Data Protection

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.

2.1 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:

2.2 Data means information in a form that can be processed. It includes both automated data (for example, electronic data) and manual data. Automated data means any information on a 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.

2.3 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.

2.4 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, that is, the school.

2.5 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.

2.6 Data controller for the purpose of this policy is the Board of Management, BOM, of [Canal Way Educate Together National School](#).

3. Rationale

In addition to its legal obligations under the broad remit of educational legislation, [Canal Way Educate Together National 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 are 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.

4. Related Documentation, 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 pupil, 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 student 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 student 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, for example, a dental inspection.
- Under Children First: National Guidance for the Protection and Welfare of Children 2011, published by the Department of Children and Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to Tusla - the Child and Family Agency, or in the event of an emergency and the unavailability of Tusla, to An Garda Síochána.

5. Relationship to characteristic spirit of the school:

[Canal Way](#) Educate Together National School seeks to enable each student to develop their full potential;

- provide a safe and secure environment for learning; and
- 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.

6. 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, 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, subjects, etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES child protection procedures)
- Details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress.

(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; and 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 or electronic database, 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.

Canal Way Educate Together use Aladdin as our 'administration system'. We store staff contact information which is necessary in order to communicate and contact trace. Appendix 1

(d) Security: There is a mix of manual and electronic records. Manual records are stored in a locked filing cabinet. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place.

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
- whether English is the pupil's first language and/or whether the pupil receives English language support
- any relevant special conditions, for example, 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 pupil
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of pupils, including at school events and noting achievements
- Academic records – class assignments, assessment 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
- 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, for example, records of any serious injuries/accidents, etc. (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 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 enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents/guardians 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, compile yearbooks, establish a 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 class
- 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 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 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.

Canal Way Educate Together use Aladdin as our 'administration system'. We store student pupil information on Aladdin which is necessary in order to pass on to government agencies for inclusion on the Primary Online Data Base, attendance for TUSLA, and report writing and communication with our community. Appendix 1

(d) Security: There is a mix of manual and electronic records. Manual records are stored in a locked filing cabinet. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place.

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.

(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.

(e) Security: There is a mix of manual and electronic records. Manual records are stored in a locked filing cabinet. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place.

D. Other records: 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.

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: There is a mix of manual and electronic records. Manual records are stored in a locked filing cabinet. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place

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
- email 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 (CHY3 or 4) 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: There is a mix of manual and electronic records. Manual records are stored in a locked filing cabinet. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place.

CCTV images/recordings

(a) Categories: CCTV The following will apply:

- a. Monitoring of the external boundaries of the school, that is, perimeter walls/fencing including the yard.
- b. Internally-corridors and foyer.
- c. These CCTV systems may record images of staff, students and members of the public who visit the premises.
- D. Staff to be made aware of location of the cameras

(b) Purposes: Safety and security of staff, students and visitors and to safeguard school property and equipment.

(c) Location: Cameras are held in classrooms and office space. They are cleared and removed over the summer months.

(d) Security: Access to images/recordings will be restricted to the Principal, Deputy Principal and School Secretary of the school. Hard drive recordings will be 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.

Assessment results

(a) Categories: The school will hold data comprising assessment results in respect of its students. These will include standardised tests.

(b) Purposes: The purpose for which these results and other records are held is to monitor a pupil's progress and to inform teaching and learning. 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.

(d) **Security:** There is a mix of manual and electronic records. Manual records are stored in a locked filing cabinet. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place

7. Links to other policies:

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
- Enrolment Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE, etc.

8. 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.

9. Dealing with data access requests:

9.1 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.

9.2 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 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.

9.3 Providing information over the telephone

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.

10. Implementation arrangements, roles and responsibilities:

In [Canalway ETNS](#), 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 staff:	Awareness of responsibilities
Administrative staff:	Security, confidentiality
ICT personnel:	Security, encryption, confidentiality

11. Ratification and communication:

When the Data Protection Policy has been ratified by the School Manager, it becomes the school's agreed Data Protection Policy. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on pupils, staff and others in the school community.

Parents/guardians and pupils should be informed of the Data Protection Policy from the time of enrolment of the pupil, for example, by including the Data Protection Policy as part of the enrolment pack, by either enclosing it or incorporating it as an appendix to the enrolment form. Parents/guardians will also be directed to the policy section of the school website.

12. Monitoring and policy implementation:

The implementation of the policy shall be monitored by the Principal and the Board of Management.

A note as part of a Report to the School Community will be issued by the Board of Management to confirm that the actions/measures set down under the policy are being implemented.

13. Review and policy evaluation:

The policy shall be reviewed and evaluated at certain times and as necessary. Ongoing review and evaluation shall take cognisance of changing information or guidelines, for example, from the Data Protection Commissioner, Department of Education and Skills or the [National Education Welfare Board](#), legislation and feedback from parents/guardians, pupils, school staff and others. The policy shall be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Signed:

Date:

Signed:

Date:

Contact details:

The Principal
Canal Way Educate Together National School,
Basin Street Upper,
Dublin 8.
Co. Dublin.
Telephone: 01 4021418
E-mail: principal@canalwayetns.org

Appendix 1

Aladdin Data Processing Agreement

(A) You, the Data Controller have entered into a Service Agreement with CLOUDWARE LIMITED T/A Aladdin Schools, the Data Processor, for the purposes of the Data Processor providing you with software services to support the management and administration of schools.

(B) You and the Data Processor are entering into this Data Processing Agreement to ensure compliance with current Data Protection Law (as applicable) in relation to all such processing.

(C) The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data processed by the Data Processor in relation to all such processing whether such personal data is processed at the date of the Service Agreement or received afterwards.

1. Interpretation

The terms and expressions set out in this agreement shall have the following meanings:

"Data Protection Law"	shall mean EU Regulation 2016/679 (GDPR) and such other applicable law which may apply
"Service Agreement"	the Terms of Service agreed between the parties for software services.
"Data Controller", "Data Processor" and "processing"	shall have the meanings given to them in Data Protection law;
"ODPC"	means the Office of the Data Protection Commission, Ireland;
"personal data"	shall include all data relating to individuals which is processed by the Data Processor on behalf of the Data Controller in accordance with this Agreement.

It is agreed as follows:

2. This Agreement sets out various obligations in relation to the processing of data under the Service Agreement. If there is a conflict between the provisions of the Service Agreement and this Agreement, the provisions of this Agreement shall prevail.
3. The Data Processor is to process personal data received from the Data Controller only on the written instructions of designated contacts at the Data Controller (which may be specific instructions or instructions of a general nature as set out in the Service Agreement or as otherwise notified by the Data Controller to the Data Processor (during the term of the Service Agreement).
4. The Data Controller warrants that at all times it shall comply with the Data Protection Law and shall not perform its obligations under this Agreement (or the Service Agreement) in such way as to cause the Data Processor to breach any of its applicable obligations under the Data Protection Law.
5. The Data Processor warrants that at all times it shall comply with the Data Protection Law and shall not perform its obligations under this Agreement (or the Service Agreement) in such way as to cause the Data Controller to breach any of its applicable obligations under the Data Protection Law.

6. All personal data provided to the Data Processor by the Data Controller or obtained by the Data Processor in the course of its work with the Data Controller is strictly confidential and may not be copied, disclosed or processed in any way without the express authority of the Data Controller.

7. The Data Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation from time to time in force and any best practice guidance issued by the ODPC.

8. Where the Data Processor processes personal data on behalf of the Data Controller it shall:

- **8.1** process the personal data only to the extent, and in such manner, as is necessary in order to comply with its obligations under the Service Agreement, or as is required by law or any regulatory body including but not limited to the ODPC;
- **8.2** implement appropriate technical and organisational measures and take all steps necessary to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from the Data Controller;
- **8.3** if so requested by the Data Controller (and within the timescales required by the Data Controller) supply details of the technical and organisational systems in place to safeguard the security of the personal data held and to prevent unauthorised access;
- **8.4** notify the Data Controller should any data security breach occur in the Data Processor's company;
- **8.5** notify the Data Controller (within two working days) if it receives:
 - **8.5.1** a request from a data subject to have access to that person's personal data;
 - or
 - **8.5.2** a complaint or request relating to the Data Controller's obligations under the Data Protection Law;
- **8.6** provide the Data Controller with full co-operation and assistance in relation to any complaint or request made, including by:
 - **8.6.1** providing the Data Controller with full details of the complaint or request;
 - **8.6.2** complying with a data access request within the relevant timescale set out in the Data Protection Law and in accordance with the Data Controller's instructions;
 - **8.6.3** providing the Data Controller with any personal data it holds in relation to a data subject (within the timescales required by the Data Controller);
 - **8.6.4** providing the Data Controller with any information requested by the Data Controller;
- **8.7** not process personal data outside the European Economic Area without ensuring there is an adequate level of protection to any personal data that is transferred,
- **8.8** not transfer any personal data provided to it by the Data Controller to any third party without the prior approval of the Data Controller, such prior approval having been provided for through the Data Controller's acceptance of the Terms of Service.
- **8.9** shall ensure that any third party to which it sub-contracts any processing has entered into a written contract with the Data Processor which contains all the obligations that are contained in this Agreement and which permits both the Data Processor and the Data Controller to enforce those obligations.

9. The Data Processor shall transfer all personal data to the Data Controller in compliance with the requirements notified in writing by the Data Controller to the Data Processor from time to time.

10. The Data Processor shall assist the Data Controller with ensuring compliance with Articles 32 to 36 of the GDPR (relating to security of personal data and risk assessments).

11. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the Data Protection Law.

12. The Data Processor warrants that it will only engage trained, competent and reliant staff to process the personal data on behalf of the Data Controller.

13. The Data Processor shall be liable for each and every action, proceedings, liability, cost, claim, loss, expense and demand incurred by the Data Controller which arise directly or in connection with the Data Processors or sub-processors data processing activities under this Agreement.

14. The Data Processor agrees that in the event that it is notified by the Data Controller that it is not required to provide any further services to the Data Controller under this Agreement, the Data Processor shall transfer a copy of all requested information (including personal data) held by it in relation to this Agreement to the Data Controller, and/or, at the Data Controller's request, destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the Data Controller with a written confirmation of secure disposal.

15. All copyright, database right and other intellectual property rights in any personal data processed under this Agreement (including but not limited to any updates, amendments or adaptations to the personal data by either the Data Controller or the Data Processor) shall belong to the Data Controller. The Data Processor is licensed to use such data only for the term of and in accordance with this Agreement.

16. The Data Processor accepts the obligations in this Agreement in consideration of the Data Controller continuing to use its services.

17. This Agreement shall be governed by the laws of Ireland.

SCHEDULE 1

DESCRIPTION OF THE TRANSFER

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

- Students
- School Staff
- Parents

Purposes of the transfer(s)

The transfer is made for the following purposes:

- To carry out the terms of the Service Agreement

Categories of data

The Personal Data transferred concern the following categories of data:

- Personal Data and Sensitive Personal Data, including without limitation:
- Students: Names, addresses, dates of birth, PPS numbers, health information, information relating to family
- Parents: Names, contact details
- School Staff: Names, work email addresses.:

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

- Only those Aladdin staff who require access to the personal data to fulfil the terms of the Service Agreement.

Additional useful information:

Data will only be retained by Aladdin for as long as is required by law, or as long as is necessary to fulfil the terms of the Service Agreement, whichever is longer.

Contact points for data protection enquiries:

Data Protection Manager

dpm@aladdin.ie

This agreement was last updated on 25th April 2018