# Data Protection Policy
## SCOIL MHUIRE, CLONDRA

**INTRODUCTORY STATEMENT**
The school's Data Protection Policy applies to the personal data held by the school's Board of Management (BoM), which is protected by the Data Protection Acts 1988 to 2018 and the EU General Data Personal Regulation (GDPR). This policy was reviewed in February 2021 in light of Covid-19 which had necessitated increased use of online communications such as e-mail (parents) and the Seesaw learning platform (pupils). Further reviewed in April 2023. This current review takes place in April 2025.

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 special categories of personal data will be protected by the school

Scoil Mhuire, Clondra will operate 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 BoM 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 Board of Management 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 a pupil's previous school/s. 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.

**2. Consent**
Where consent is the basis for provision of personal data (e.g. data required to join sports team/ after-school activity or any other optional school activity) the consent must be a freely given, specific, informed and an unambiguous indication of the data subject's wishes. Scoil Mhuire Clondra 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

**3. Keep it only for one or more specified and explicit lawful purposes**
The Board will inform individuals of the reasons they collect their data and 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 information. Personal data is securely stored under lock and key in the case of manual records and protected with computer software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) are password-protected.

**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. 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 information 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 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. We will be informed by CPSMA document 'Data Retention Periods for Schools' (Appendix A).

**9. Provide a copy of their personal data to any individual on request**
Individuals have a right to know and have access to a copy of personal data held about them, by whom, and the purpose for which it is held. Individuals can apply to the Board of Management for such information using a Personal Data Access Request form (Appendix B).

**SCOPE**
The Data Protection legislation applies to the keeping and processing of personal data. 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:

*Personal Data* means any data relating to an identified or identifiable natural person i.e. 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 (BoM).

*Data Controller* is the Board of Management of the school.

*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. We use Aladdin school management software to store and process information.

*Special categories of personal data* refers to personal data regarding a persons'

- racial or ethnic origin
- political opinions or religious or philosophical beliefs
- physical or mental health
- sexual life and sexual orientation
- genetic and biometric data
- criminal convictions or the alleged commission of an offence
- trade union membership

*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 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. 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. Scoil Mhuire, Clondra sends, by post, a copy of a child's Education Passport, as provided by the National Council for Curriculum and Assessment, to the Principal of the Post-Primary School in which the pupil has been enrolled.

Where reports on pupils which have been completed by professionals, apart from Scoil Mhuire staff, are included in current pupil files, such reports are only passed to the Post-Primary school following express written permission having been sought and received from the parents of the said pupils.

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, Tusla, the National Council for Special Education and other schools). The Board must be 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; 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) 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 most schools are not currently subject to freedom of information legislation (with the exception of schools under the direction of Education and Training Boards), 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 by that body 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 Act 2015***, mandated persons in schools have responsibilities to report child welfare concerns 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 Mhuire, Clondra, seeks to:

- enable students 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 legislation.

**PERSONAL DATA**
The personal data records held by the school **may** include:

***1. 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.
- Name and contact details of next-of-kin in case of emergency.
- 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 Children First Act 2015.

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 and Security procedures of Scoil Mhuire:*

a. Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
b. Digital records are stored on password-protected computer in a locked office. The school has a burglar alarm which is activated during out-of-school hours.

## *2. **Student records:***

*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, e-mail addresses 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
- Individual Administration of Medicines Policies on children who may need medication during the school day.
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements) are managed in line with the accompanying policy on school photography.
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports. Pupil work and records will also be stored and archived on the Seesaw platform.
- 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 Children First Act 2015.

*b) Purposes: The purposes for keeping student records include:*

- to enable each student to develop to his/her 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, e.g. compile yearbooks, 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 Photography Policy'* and '*School Website Privacy Statement'*.
- to ensure that the student meets the school's admission criteria

- to ensure that students meet the minimum age requirement for attendance at Primary School.
- 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 second-level educational institutions.

*c) (Location and Security procedures - as above)*

***3. Board of Management records:***

*a) Categories of Board of Management data:*
- 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 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 and Security procedures - as above)*

***4. Other Records: Creditors***

*a) Categories of Board of Management 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: The purposes for keeping creditor records are:*
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 and Security procedures - as above)*

***5. Other Records:***
It is also necessary for the school to store other information such as school accounts, copies of tax and revenue returns on ancillary staff, etc. This information is necessary in order to comply with our statutory obligations and for the routine management and administration of the school's financial affairs.

**EXAMINATION RESULTS**

The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual and continuous assessment results and the results of Standardised Tests

***Purposes:***

The main purpose for which these examination results are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardian about educational attainment levels and recommendations for the future. 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 other schools to which pupils move.

***Location and Security procedures***

As above

**Aladdin School Management System**

One of the IT service companies that we use includes Cloudware Limited (T/A Aladdin Schools) ('Aladdin'). Aladdin processes personal data on behalf of the school in order to provide an online management information system.

Anyone provided with a username and password and who is authorised to use the Aladdin system by the school should adhere to and be aware of the following:

- users may be allocated different access rights to the Aladdin system. The access rights are solely determined by the school. If you have any concern over the access rights that you have please contact the Aladdin school liaison;
- a log is taken of some actions undertaken by the user when using the Aladdin system and made available to the school;
- a unique username and password is provided to each user. Users should keep their username and password confidential and not disclose it to anybody or allow any person to access the system using their username and password;
- the Aladdin system should only be used for the purposes of managing internal school administration activities and for no other purpose. The Aladdin system should not be accessed in the event of suspension or termination of the users position at the school.The school is responsible for ensuring that access to the Aladdin system for terminated or suspended users is disabled;
- each user should ensure they are familiar with the Aladdin system before use. All queries should be referred to the Aladdin liaison person mentioned above;
- the user should notify the Aladdin administrator in the event of any misuse or loss of their username and password;
- the user should only login to the Aladdin system when in a secure and non-public environment, e.g. the school or home of the user;
- the user should sign out of the Aladdin system or lock their device when leaving the device unattended
- the Aladdin system should not be used to deal with emergency situations and it should not be relied upon during such times;
- users are responsible for ensuring that all communications sent to parents or guardians using the Aladdin system are accurate and are sent to parents/guardians for whom the school has appropriate and up to date consent and contact details;
- before each communication, users should consult with the appropriate school's database to determine which parents or guardians have consented to being contacted;

- the Aladdin system should not be accessed through an unsecure network or internet connection. If in doubt, the user should wait until in a secure environment before accessing the Aladdin system;
- information available through the Aladdin system should only be printed or saved to an electronic device where absolutely necessary. Any hardcopy or electronic files originating from the Aladdin system should be treated in accordance with the relevant provisions of this policy; and
- users may be able to access the websites of other third party service providers when accessing the Aladdin system. When the user accesses a third party website from the Aladdin system they are leaving the Aladdin system and appropriate due diligence should be undertaken before sharing any personal data with that third party. The Aladdin liaison person should be contacted if the user is in any doubt.

**SEESAW**

In March 2020, having researched online learning options, we decided to use the Seesaw platform to communicate with pupils. In September 2020 we purchased the 'Seesaw for schools' licence in order to engage with pupils who may have to isolate or in case of further schools closure. Seesaw is compliant with EU GDPR legislation. Although we have discontinued use of this platform, it may be used in the future.

Parental consent will be obtained for every child accessing our Seesaw portal.

See appendix D: Seesaw privacy policy.

**ZOOM**

Rules governing the use of Seesaw also apply to the Zoom platform. Our Remote Teaching and Learning Plan also covers the use of Zoom as an online tool.

Parent's e-mails may be used to inform them of Zoom meetings. Meetings will not be recorded.

Staff conducting Zoom meetings are aware of the risk of hacking/intrusion on meetings. They will respond by ending the meeting immediately.

Parents and staff are aware of our Remote Teaching and Learning Plan which explicitly disallows the sharing by pupils, parents, teachers, or administrators using online platforms such as Seesaw and Zoom, any content outside of the platform whether on social media or by any other means, electronic or concrete.

**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:

- General School Policy
- Pupil Online Database (POD): Collection of the data for the purposes of complying with the Department of Education and Skills' pupil online database.
- Child Protection Procedures
- Anti-Bullying Procedures
- Code of Behaviour
- Enrolment Policy
- ICT Acceptable Usage Policy
- Assessment Policy
- Special Educational Needs Policy
- Critical Incident Policy
- Attendance Policy

**PROCESSING IN LINE WITH A DATA SUBJECT'S RIGHTS**

Data in this school will be processed in line with the data subject's rights. Data subjects have a right to:

- Know what personal data the school is keeping on them
- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Ask to have data erased once it is no longer necessary or irrelevant.

***Data Processors***

Where the school outsources to a data processor off-site, it is required by law to have a written contract in place. Scoil Mhuire's third party agreement specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data must be deleted or returned upon completion or termination of the contract. See Appendix C.

***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 request***

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

Request must be responded to within one month. An extension may be required e.g. over holiday periods

No fee may be charged except in exceptional circumstances where the requests are repetitive or manifestly unfounded or excessive

No personal data can be supplied relating to another individual apart from the data subject. If a document concerning information on the data subject also contains information on another person then it should be redacted.

**PROVIDING INFORMATION OVER THE PHONE**

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

- Verify the caller's identity.
- Ask that the caller put their request in writing
- Refer the request to the Principal for assistance in difficult situations
- Not feel forced into disclosing personal information

**IMPLEMENTATION ARRANGEMENTS, ROLES AND RESPONSIBILITIES**

The BoM is the data controller and the Principal implements the Data Protection Policy, 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 |

**MONITORING THE IMPLEMENTATION OF THE POLICY**

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

**REVIEWING AND EVALUATING THE POLICY**

The policy will be reviewed and evaluated after 2 years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g., from the Data Protection Commissioner, Department of Education and Skills or TUSLA), legislation and feedback from parents/guardians, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning

This Policy was ratified by the Board of Management of Clondra National School on:

_____

Signed: _____

Mrs Mary Duignan, Chairperson, Board of Management, Scoil Mhuire Clondra

*Appendix A*

*Appendix B*

**Personal Data Access Request Form**

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

**Important: 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: | |

I, …… [name] wish to make an Access Request for a copy of personal data that Scoil Mhuire, Clondra 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, and any other information relevant to your access request

| |
|---|
| |

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:<br>**To the Chairperson of Board of Management, Scoil Mhuire, Clondra, Co Longford.** |

*Appendix C*

## Data Processing agreement with Aladdin Schools

(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 Officer
dpo@aladdin.ie
This agreement was last updated on 25th April 2018

## ***Appendix D: Seesaw Privacy Policy***

*Effective Date: September 3, 2019*

*INTRODUCTION*

Seesaw's mission is to create an environment where students can be their best. To accomplish this goal, it's essential that Seesaw is a safe place for students to document their learning, and that families and teachers are in complete control over how that information is shared.

Protecting your privacy is fundamental to our mission and business. The following summarize our promises to you.

- We never sell your data or student data.
- We never advertise in Seesaw.
- We don't own the content you add to Seesaw.
- Student work is private to the classroom by default.
- We use the latest security industry best practices to protect you.
- We are transparent about our practices and will notify you if things change.
- We are compliant with FERPA, COPPA, GDPR, MFIPPA, and the Australian Privacy Act.

You can read more about our Privacy Principles and our commitment to privacy here.

This Privacy Policy governs the use of data collected by our websites at seesaw.me, and the Seesaw Application (collectively "the Seesaw Service", "the Service" or "Seesaw"). This includes personally identifiable information that we collect when you create an account ("Account Information"), content added to class journals ("Journal Content"), Activities teachers create, and Messages sent via Seesaw. Any data collected by Seesaw that can be linked back to an individual student is considered "Student Data".

By using Seesaw, you agree to this Privacy Policy. If you don't agree, please don't use Seesaw. You can contact us anytime with questions about this policy at help@seesaw.me.

*SEESAW AND PARENTAL CONSENT*

We require that teachers or schools get parental consent before using Seesaw with children who are under the age when they can grant consent on their own. This age may vary based on where you live. For example, in the US that age is younger than 13. You should check your local laws to determine the relevant age in your country. Parents or guardians can withdraw consent for the further collection of their child's information at any time. If you are aware Seesaw is collecting information from a student without parental consent, please contact us immediately at help@seesaw.me and we will delete the data.

There are a number of ways in which teachers or schools can obtain parental consent:

- Get consent as part of a school-wide technology consent process you may already have in place.
- Use our sample consent form - but please note that this is an example only and does not constitute legal advice.
- For teachers in the United States, agree to act as the parent's agent, and provide consent on their behalf to use Seesaw solely in the educational context as provided by the FTC. Learn More.

*SEESAW AND FERPA*

Data collected by Seesaw may include personally identifiable information from education records that are subject to the Family Educational Rights and Privacy Act, "FERPA", ("FERPA Records"). To the extent that Student Data includes FERPA Records, you designate Seesaw as a "School Official" (as that term is used in FERPA and its implementing regulations) under the direct control of the school with regard to the use and maintenance of the FERPA Records and Seesaw agrees to comply with FERPA.

*SEESAW AND GDPR*

Seesaw complies with the European Union General Data Protection Regulation (the "GDPR") and makes it easy for EU individuals to exercise their rights described in that regulation. The purposes for which Seesaw collects your information, the categories and specific types of information, and our practices and policies regarding the processing of your information are described in this Privacy Policy and our Data Processing Agreement. If you have specific questions about how Seesaw is compliant with GDPR, please see our frequently asked questions about GDPR.

*WHO DOES SEESAW COLLECT INFORMATION FROM?*

Teachers, parents, family members, students, and schools may create accounts on Seesaw. We also collect limited log-data from all visitors to our marketing website.

*WHAT INFORMATION DOES SEESAW COLLECT?*

**Account Information:** When teachers, parents, family members, or school administrators create an account on Seesaw we collect your name, email address, password, and profile picture. Seesaw may also collect your phone number if you enter it in your Account Settings.

Teachers using Seesaw to communicate with Families may add a family member's email or phone number to Seesaw in order to send messages or updates about school work to the appropriate parent or family member.

Students cannot create an account by themselves, but must be invited to a Seesaw class by a teacher or school administrator. Where students have permission to use Seesaw, Seesaw collects personally identifiable information about them including their names, email addresses, and profile picture. This information may be entered by a teacher or the student or populated from the student's account with a third party sign-in service, such as their Google account.

**Journal Content:** Seesaw also collects content that is added to a class or student journal. This content may be photos, drawings, files, notes, hyperlinks, and other ways of documenting student learning. We regularly add types of information that can be uploaded to a Journal, and these are all covered by this Policy. We also collect comments on posts in your class journal which may be text, or if you allow Seesaw to access the microphone on your device, voice recordings. Journal Content that is uploaded by a student or teacher may be considered a student education record as defined by FERPA.
**Messages:** Seesaw collects messages that are sent and received in Seesaw by teachers, family members, and students.
**Activities:** Teachers may use Seesaw to create activities to use with their students. Activities may include text or voice instructions for how to complete the activity, an example of a correct response or a template for students to edit.
**Activity Author Profiles:** Teachers who choose to publish activities to the Community Activity Library or the Activity Library managed by their school or district can also create an Activity Author Profile. This includes the name and profile picture they choose to publish on their Author Profile, as well as their school name and location.
**Communications:** Seesaw collects any information you send to us directly, such as email communications.
**Information from your Google Account or other Third-Party Sign-in Service:** Seesaw allows teachers, parents, family members, and students (after being invited by a teacher) to sign up for and log into our service using a Google or Clever Account. Teachers can also create student accounts on behalf of students in their class. When we create a Seesaw account using one of these Third-Party Services, we use the name, profile picture, and email address (if available) provided by these services.
**Log Data:** When you use Seesaw, we receive log data such as your IP address, browser type, operating system, device information, and your mobile carrier. In addition, we may receive or collect additional information such as the referring web page, referring search terms, and pages visited. If you are using Seesaw as a teacher, parent, or administrator, Seesaw may use your IP address to determine your approximate location for the purposes of sending you customized marketing and other information about our products.

*HOW DOES SEESAW USE THIS INFORMATION?*
We only use this information to provide our services to you. For example we use this information to:

- Allow you to access and use our service by verifying your identity and storing your Journal Content, Activities, and Messages.
- Provide teachers, schools, and family members with customer support.
- Notify you about activity on and updates to your account or your child's account (if you've indicated in your account settings that you'd like notifications).
- Research, understand, and analyze trends of users to improve and develop new features for our products.
- Promote enhancements to Seesaw relevant for teachers, families and schools.
- Investigate, prevent, and detect activities on our service that we believe may violate the law or applicable regulations. We may, at the request of a school, investigate accounts to determine whether they comply with school policies.

You can withdraw consent for the collection of your personal information at any time, and also opt-out of marketing communications from us.
*DOES SEESAW ALLOW ADVERTISING OR SHARE DATA FOR ADVERTISING?*
Absolutely not. Our business model is straightforward: we charge for optional, additional features on top of our free product and have no interest in advertising within Seesaw. We never display ads, allow third-party ads, share data for advertising or marketing purposes, or allow data collection by third-party advertisers or data brokers. We do not allow in-app purchases for student accounts.

*IN WHAT LIMITED CIRCUMSTANCES MAY SEESAW NEED TO SHARE MY INFORMATION?*
We do not sell or share any data you provide with third parties except in the limited circumstances detailed below:

- We use a small number of third-party services in order to operate and improve Seesaw – for example a data center operator that manages our servers or a notification service that helps us send you messages about your account. These services need access to your personally identifiable information in order to work (i.e. your email address is required to send you email), but are contractually prohibited from using that information for any other purpose other than to provide the Seesaw service. In cases of onward transfer to third parties of data of EU individuals received pursuant to the EU-US and the Swiss-US Privacy Shield, Seesaw is potentially liable. A list of the third-party services that obtain personally identifiable information we currently use can be found here. When these third-party services transfer the personal information (Personal Data, as that term is defined in GDPR) of EU residents, these services are processors and are contractually bound to also comply with GDPR to protect your data privacy and security.
- Seesaw may disclose your information to a third party to comply with applicable laws or regulations, or a valid legal request - including to meet national security or law enforcement requirements. If we are going to release your data, we will do our best to provide you with notice in advance by email, unless we are prohibited from doing so by law.
- Seesaw may disclose student Account Information and Journal Content to the child's school district upon request, as required by FERPA.
- By default Activities teachers create are private to their account. Optionally, teachers may choose to publish Activities they create to the Community Activity Library or the Activity Library managed by their school or district. In these cases, the activity and the teacher's Activity Author Profile will be shared publicly (in the case of

the Community Library) or with other teachers at their school or district. No student responses to Activities are ever shared.

- We may share activities published to the public Community Activity Library with teachers who we think may be interested in using them with their class.
- We may disclose or transfer your Account Information and Journal Content in connection with the sale, merger, bankruptcy, sale of assets or reorganization of our company. We will notify you if a different company will receive your information. The promises in this Privacy Policy will apply to your data as transferred to the new entity.

*DO YOU COLLECT DATA ABOUT [BLANK]?*

We've listed all the data we collect in the section above titled What Information Does Seesaw Collect. We intentionally limit our data collection to only what we need to provide the Seesaw service for you.

However, sometimes we get asked if we collect data about some other topic or area that's of particular interest to a school. To be clear, we do not collect biometric, behavioral, free or reduced lunch eligibility, health, or financial data.

*DO YOU WORK WITH THIRD-PARTY ANALYTICS SERVICES?*

Seesaw is constantly improving, and we use aggregate data about how Seesaw is used -- for example what buttons you click on or what pages you visit -- to inform those decisions.

To help us analyze this data, we use a small number of third-party services (such as Google Analytics). In no circumstances are any data you have shared with Seesaw (such as your Account Information or Journal Content) shared with these services. In addition, these services are contractually obligated only to use data about your usage of Seesaw to provide analytics services to us and are prohibited from sharing it or using it for other purposes. If you do not wish to participate in Google Analytics, you may download the Google Analytics opt-out browser add-on.

*HOW DO YOU USE COOKIES?*

Cookies are small text files that we transfer to your web browser that allow us to identify your web browser and store information about your account. We use these cookies to keep you logged in to Seesaw, customize your Seesaw experience, understand how you use Seesaw, and promote Seesaw to relevant teachers and schools.

You can choose to remove or disable cookies via your browser settings. Please be aware that Seesaw will not work properly if you disable or decline cookies.

*HOW CAN USERS SHARE STUDENT AND CLASS JOURNAL INFORMATION?*

Seesaw is designed to promote safe sharing. Teachers control who can see Messages or access a student's Journal Content by authorizing specific people to connect to that student's account. Teachers may also choose to publish some class content to a public class web page managed by Seesaw.

Teachers also control whether or not students or family members can save Seesaw content to their device or get a link to specific Journal Content. However, it's worth noting that we cannot prevent all forms of sharing (e.g. by taking a screenshot) so it's important that Teachers only grant access to their class to authorized parties.

*HOW DOES SEESAW HANDLE ABANDONED ACCOUNTS?*

Seesaw will delete an account and all content associated with the account if the account has not been accessed for more than 7 years. Prior to deleting an abandoned account, Seesaw will notify the teacher or school associated with the account by email and provide an opportunity to download an archive copy of the class journal.

*HOW TO VIEW, CORRECT, EDIT, PORT, OR UPDATE YOUR PERSONAL INFORMATION*

You have the right to access, correct, download for transport to a similar service, or delete any of your personal information collected by Seesaw. If you are a parent or teacher, you can update the information associated with your Seesaw account directly by logging into your Seesaw account and viewing the Account Settings tab on your profile. If you are a parent and want to correct, edit, download, or update information about a student, please work directly with your teacher or school, or you can contact us at help@seesaw.me.

*HOW TO DELETE YOUR SEESAW ACCOUNT*

If you would like to delete your Seesaw account or any content submitted to Seesaw, please send an email to help@seesaw.me. If you request that your account or any content submitted to Seesaw be deleted, Seesaw may still retain information for up to 60 days to provide customer support and prevent accidental deletion.

If you are a teacher or school administrator within the US, please be aware that FERPA requires us to retain student education records once a valid request to inspect those records has been made.

*HOW DOES SEESAW KEEP YOUR DATA SAFE?*

Seesaw takes protecting your security and privacy seriously and we've put a number of measures in place to protect the integrity of your information, including use of access-controlled data centers, routine 3rd party security audits, restricted employee access to user information, data encryption in transit and encryption of Journal Content at rest. For more information, please read this article.

In the event of a security breach, we will notify affected account holders within the amount of time required by law so that you can take steps to keep your data safe.

*HOW DOES SEESAW HANDLE DATA FROM INTERNATIONAL VISITORS?*

The Seesaw Service is hosted and operated in the United States and is subject to United States law. By default, any personal information that you provide to Seesaw will be hosted on servers located in the United States. By using this Service, you consent to the transfer to and processing of your personal information in the United States. If your school or district has purchased Seesaw for Schools, your school or district can choose to store all data associated with your Seesaw for Schools account in a different supported country. By participating in Seesaw for Schools you consent to allow your school or district to determine where to store all your data. Please contact your Seesaw for Schools administrator to find out where your data is stored.

Seesaw complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from the European Union. the United Kingdom, and Switzerland transferred to the United States pursuant to Privacy Shield. Seesaw has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Seesaw is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Seesaw's accountability for personal data that it receives in the United States under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. Pursuant to the Privacy Shield, Seesaw remains liable for the transfer of personal data to third parties acting as our agents unless we can prove we were not a party to the events giving rise to the damages.

In compliance with the Privacy Shield Principles, Seesaw commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union and Swiss individuals with Privacy Shield inquiries or complaints should first contact Seesaw by email at privacy@seesaw.me.

Seesaw has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

*DOES SEESAW COMPLY WITH YOUR STATE'S LAWS?*

We sometimes get asked whether Seesaw complies with specific US state laws. For more information about your state, please see here.

*RIGHTS OF CALIFORNIA RESIDENTS*

If you are a California resident, please see here for more information about our practices and your rights with respect to your information.

*CHANGES TO OUR PRIVACY POLICY*

Seesaw may from time to time make changes to this Privacy Policy to account for changes to our practices or applicable law. If we make changes to this Privacy Policy that we believe will materially affect your rights, we will notify you by email about these changes and post a notice to our service. If you continue to use our service after you receive notice of changes to this Privacy Policy, you will accept these changes.

*CONTACT INFORMATION*

If you have any questions about this Privacy Policy or feedback, please contact help@seesaw.me. You can reach Seesaw by mail at:

Seesaw Learning, Inc.
180 Montgomery Street, Suite 750
San Francisco, CA 94104