

Scoil Náisiúnta Ros Eó,
Ros Eó,
Co. Bhaile Átha Cliath.
K56 VK88
Guthán : 01 843 7095
Facs. 01 843 7095
Email: rushns.ias@eircom.net
Website: www.rushnationalschool.ie
R.C.N: 20119270



Rush National School,
Rush,
Co. Dublin.
K56 VK88
Tel: 01 843 7095
Fax. 01 843 7095
Email: rushns.ias@eircom.net
Website: www.rushnationalschool.ie
R.C.N: 20119270

Data Protection Policy

Introductory Statement

This Data Protection Policy was devised and formulated by the school community, involving Board of Management, parents and staff of Rush National School, in accordance with the Rules and Regulations of the Department of Education and Skills and the Catholic Primary Schools Management Association. This policy has been informed by the Data Protection in Schools website, the Data Protection Commissioner website, the General Data Protection Regulation 2018 and the Irish Primary Principals' Network.

This Data Protection Policy applies to the personal data held by Rush National School and is underpinned by the Data Protection Acts 1988 to 2018, the European Union Data Protection Directive 95/46/EC and the European Union General Data Protection Regulation 2018. The policy applies to all school staff, the Board of Management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Rush National School operates a "Privacy by Design" method in relation to Data Protection. This means we plan carefully when gathering personal data so that we build in the data protection principles as integral elements of all data operations in advance.

We audit the personal data we hold in order to:

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

Ethos

Rush National School is a co-educational primary school, which strives to provide a well ordered, caring, happy and secure atmosphere where the intellectual, spiritual, physical, moral and cultural needs of the pupils are identified and addressed. While respect is paid to all religious and/or value systems, Rush National School is a Catholic school under the patronage of the Archbishop of Dublin.

Compliance with School Ethos

Rush National School seeks to enable each student to develop their full potential, to provide a safe and secure environment for learning and to promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society. Rush National School aims to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with the school. Rush National School wishes to achieve these aims while fully respecting individuals' right to privacy and rights under the Data Protection Acts 1988 to 2018 and the European Union General Data Protection Regulation 2018.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, Rush National School has a legal responsibility to comply with the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2018. 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. A copy of Rush National School's Record Retention Schedule is found in Appendix 7.

Rush National School takes its responsibilities under Data Protection law very seriously, and wishes to put in place safe practices to safeguard individuals' 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.

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

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the school.
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply Personal Data kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board (from 1/01/2014 known as TUSLA- The Child and Family Agency), 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) 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 a 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 (or in the event of an emergency and the unavailability of Tusla, to An Garda Síochána).

General Aim

The Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2018 apply to the keeping and processing of personal data, both in manual and electronic form. The purpose of this policy is to assist Rush National School to meet its statutory obligations, to explain those obligations to school staff and to inform staff, students and their parents/guardians on how their data will be treated.

List of Appendices

Appendix 1: Rush National School Data Protection Privacy Statement for Parents, Guardians and Pupils

Appendix 2: Rush National School Personal Data Access Request Form

Appendix 3: Rush National School Personal Data Rectification/Erasure Form

Appendix 4: Rush National School Personal Security Breach Code of Practice

Appendix 5: Rush National School Website Privacy Statement

Appendix 6: Aladdin Schools Online Management Information System Processing Agreement

Appendix 7: Rush National School Records Retention Schedule

Definition of Data Protection Terms

In order to properly understand the Rush National School’s obligations, there are some key terms which should be understood by all relevant parties:

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

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

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

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

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

Data Controller for the purpose of this policy is the Board of Management, Rush National School.

Data Protection Principles

Rush National School is a data controller of personal data relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2018 which can be summarised as follows:

- **Obtain and process Personal Data fairly:** Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts 1988 to 2018, the European Union Data Protection Directive 95/46/EC and the European Union General Data Protection Regulation 2018 and the terms of this Data Protection Policy. The information will be obtained and processed fairly.
- **Keep it only for one or more specified and explicit lawful purposes:** The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.
- **Process it only in ways compatible with the purposes for which it was given initially:** Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.
- **Keep Personal Data safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically

stored data. Portable devices storing personal data (such as laptops) should be password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- **Keep Personal Data accurate, complete and up-to-date:** Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.
- **Ensure that it is adequate, relevant and not excessive:** Only the necessary amount of information required to provide an adequate service will be gathered and stored.
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given:** As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.
- **Provide a copy of their personal data to any individual, on request:** Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

Personal Data

The Personal Data records sought and retained by Rush National School may include but are not limited to those listed below:

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
- In Case of Emergency contact
- Standard Application Forms
- 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

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

(b) Purposes

The rationale for seeking and retaining staff records is as follows:

- 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

- Principal's Office
- Principal's Hard Drive
- Esinet

(d) Security

- There is a secure, locked filing cabinet designated for individual staff files in the Principal's Office
- Where online applications are accepted they are received and stored on the relevant password protected school email account and kept in line with the recommended DES retention schedule
- Interview records for shortlisted candidates will be printed and stored in an Appointments Folder in a locked filing cabinet designated for staff files in the Principal's Office
- There is a secure, locked filing cabinet designated for the storage of substitute teacher/SNA files in the Principal's Office
- SNA Weekly Record Sheets are deposited into the Principal's office and stored in a secure, locked filing cabinet
- SNA Incident Logs are stored in a secure lockable desk. A summary document is inputted on the Aladdin Schools Online Management Information System.
- Information uploaded to Esinet is password protected.

- The Principal, Deputy Principal and School Secretary have authorised access to these files.
- Employees are required to maintain the confidentiality of any data to which they have access.

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 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 pupil
- Psychological, psychiatric and/or medical assessments
- Child Protection/ Child Welfare Records
- Attendance records
- Medical records
- Explanations pertaining to a pupil absence
- Photographs and recorded images of students (including at school events)
- Academic record – standardised test results as on official school reports
- Records of significant achievements
- Records relating to the administration of First Aid
- Whether the pupil is exempt from studying Irish
- Pupil early collection/return record files
- School Care Team records pertaining to pupils
- Student Council membership
- Special Needs Assistants' Communication Books
- Special Needs Assistants' Incident Logs
- Early Bus Departure Transport Consent Forms
- Diagnostic testing/screening results
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State Departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) Purposes

The rationale for seeking and retaining student records is as follows:

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the student
- to celebrate school achievements, 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's Data Protection Statement (Appendix 1)
- to ensure that the student meets the school's admission criteria
- to ensure that any student seeking an exemption from Irish meets the criteria to obtain such an exemption from the authorities
- To record information pertaining to health and safety
- to furnish documentation/information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other schools in compliance with law and directions issued by government departments

(c) Location

- Principal's Office
- Deputy Principal's Office
- The Secretary's Office
- Rush National School Strong Room
- Rush National School Media Drive/Teacher Share
- Aladdin Schools Online Management Information System
- Primary Online Database
- First Aid Duplicate Book
- Ipad/Tablet Storage Hub

(d) Security

- There is a secure, locked filing cabinet designated for individual pupil files in the Principal's Office
- There is a secure, locked filing cabinet designated for enrolment files in the Principal's Office
- There is a secure, locked filing cabinet, designated for files relating to Child Safeguarding in the Principal's Office*
- There is a secure, locked filing cabinet designated for all Special Educational Needs files in the Deputy Principal's Office
- There is a secure and locked strong room which hosts the archive of past pupil files
- The Rush National School Media Drive/Teacher Share which stores photographs is password protected

- The Aladdin Schools Online Management Information System which stores standardised test results and annual reports is password protected and a service user agreement is in place
- Pupil information for the Primary Online Database (POD) is inputted directly and is password protected.
- Written explanations pertaining to a pupil absence are recorded by the class teacher on the Aladdin Schools Online Management Information System and the original written explanation is immediately returned to the parent/guardian. Parents are asked to retain this for possible future use. The Aladdin Schools Online Management Information System which stores explanations pertaining to a pupil absence is password protected and a service user agreement is in place.
- Each class has a designated tablet device to take photographs/recordings of class activities. This device stays with the class throughout the class's time in the school and is password protected. In line with the Rush National School IT/AUP Policy, staff of Rush National School are not permitted to use personal devices to take photographs/recordings of class activities. These tablet devices are stored in the secure Ipad/Tablet Storage Hub
- The First Aid Duplicate Book is stored in a secure lockable filing cabinet designated for First Aid in Room 9.
- The First Aid Incident Book is stored in a secure lockable filing cabinet in the secretary's office. This is then archived in the Rush National School Strong Room
- There is a designated folder for Pupil Early Collection/Return Records in the secretary's office. These are categorised from Junior Infants to Sixth class in a designated folder per class level. Each child has a designated section for any potential occasions where they are collected early/returned during the school day. Parent(s)/Guardian(s) will sign this record.
- Archive Special Needs Assistants' Communication Books will be stored in the Rush National School strong room.
- Special Needs Assistants' Incident Logs SNA Incident Logs are stored in a secure lockable desk. A summary document is inputted on the Aladdin Schools Online Management Information System.
 - The Principal*, Deputy Principal*, School Secretary, Class Teacher and Special Needs Assistant have authorised access to these files.
 - Employees are required to maintain the confidentiality of any data to which they have access.

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 of Management
- Minutes of Board of Management meetings and correspondence to the Board of Management which may include references to particular individuals.

(b) Purposes

The rationale for seeking and retaining Board of Management records is as follows:

- 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

- Principal's Office
- Rush National School Strong Room

(d) Security

- The Board of Management Meeting records are printed and stored in a Board of Management file in a secure, locked filing cabinet in the principal's office
- Archive Board of Management files are stored in a secure and locked strong room.
- The original electronic documents (e.g. minutes) are stored on the Principal's hard drive. This file is password protected. The passwords will be made known to the Principal.
- Principal's reports emailed to the Board of Management Recording Secretary for drafting as minutes of Boards meeting will be password protected and deleted once returned to the secretary of the Board of Management.
 - The Principal and Staff Representative on the Board of Management will have authorised access to these files.
 - Employees are required to maintain the confidentiality of any data to which they have access.

Creditors

(a) Categories of Creditors' Data

Rush National School may hold some or all of the following information about creditors (some of whom may be self-employed individuals):

- name
- address
- contact details
- PPS number
- tax details
- bank details and
- amount paid.

(b) Purposes

The rationale for seeking and retaining Creditors Data is as follows:

- 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

- Secretary's Office
- Principal's Office

- Designated Assistant Principal's Room
- Rush National School Strong Room
- Assistant Principal's Room

(d) Security

- Manual record of financial transactions for the “Rush National School Main Account” and the “Rush National School Minor Works Account” are stored in a designated secure and locked filing cabinet in the Secretary's Office. The digital record is stored on a password protected hard drive of the individual responsible for the administration of the account.
- Manual record of financial transactions for the “Rush National School Book Lending Account” are stored in a designated secure and locked filing cabinet in the Principal's Office. The digital record is stored on a password protected hard drive of the individual responsible for the administration of the account.
- Manual record of financial transactions for the “Rush National School Teachers' Account” are stored in a designated secure and lockable desk in the relevant Assistant Principal's room. The digital record is stored on a password protected hard drive of the individual responsible for the administration of the account.
- Archive financial records are stored in the locked Rush National School Strong Room
 - The Principal, Deputy Principal and Secretary have authorised access to these files.
 - The relevant Assistant Principal will have access to the “Rush National School Teacher's Account”
 - Employees are required to maintain the confidentiality of any data to which they have access.

Assessment Records

(a) Categories

- Individual Class Teachers will maintain an assessment folder for their current class listing ongoing class assessments, e.g. weekly test results, teacher designed assessment tasks, portfolio material, etc.
- The school will hold data comprising of annual standardised/screening assessment results in respect of its students
- The school may administer diagnostic assessments/screening which provides the school with a more in-depth analysis of a pupil's academic progress.
- An annual school report is issued for each student.

(b) Purpose

The rationale for seeking and retaining assessment records is as follows:

- to monitor a student's progress.
- to enable each student develop to his/her potential
- to meet the educational, social, physical and emotional requirements of the student
- to furnish documentation/information 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 secondary schools (which have confirmed enrolment of the pupils concerned) with 'Education Passports'

(c) Location

- Teacher's Lockable Desk
- Principal's Office
- Copies of Annual Pupil Reports
- Aladdin Schools Online Management Information System
- Rush National School Strong Room
- Designated school laptop

(d) Security

- Each class teacher and any visiting Department of Education and Skills Inspector requires access to the class based assessment folder. These files are daily, working documents. They will be stored in the teacher's lockable desk
- There is a secure, locked filing cabinet designated for individual pupil files containing annual pupil reports in the Principal's Office
- The Aladdin Schools Online Management Information System stores standardised assessment and screening results. It is password protected and a service user agreement is in place
- Archived annual reports for past pupils will be stored in stored in the locked Rush National School Strong Room
- Diagnostic testing/screening results are uploaded to the Aladdin Schools Online Management Information System which is password protected. Information is then erased from the designated school laptop.
 - The Principal, Deputy Principal, School Secretary and Class Teacher have authorised access to these files.
 - Employees are required to maintain the confidentiality of any data to which they have access.

CCTV Images/Recordings

(a) Categories

CCTV is installed in Rush National School externally i.e. perimeter walls and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.

(b) Purposes

The rationale for seeking and retaining CCTV Images/Recordings is as follows:

- To promote and ensure the Safety and security of staff, students and visitors and to safeguard school property and equipment.

(c) Location

- Cameras are located externally and internally as detailed in the CCTV Policy.

- Image recording equipment is located in the Principal's Office.

(d) Security

- Image recording equipment is password protected
- Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2018.
 - The Principal and Deputy Principal will have authorised access to these files.
 - Employees are required to maintain the confidentiality of any data to which they have access.

Processing in Line with a Data Subject's Rights

Data in Rush National 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 called a Third-Party Service Agreement
- Rush National School'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.

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 Board of Management 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 (Board of Management) without undue delay.
- See the Rush National School Security Breach Code of Practice (Appendix 4) for more information.

Dealing with a Data 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
- 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
- Individuals should use the Rush National School Data Access Request Form (Appendix 2)

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 should:
 - 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 Board of Management 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 Rush National School Data Protection Policy:

Role of Parent

Parents/Guardians of pupils attending Rush National School must be familiar with the Rush National School Data Protection Policy and the accompanying procedures.

Role of Teacher

The teacher must be familiar with the Rush National School Data Protection Policy and the accompanying procedures.

Role of Principal

The Principal implements the Rush National School Data Protection Policy.

Role of the Board of Management

The Board of Management of Rush National School is the data controller.

Ratification, Communication and Review

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

A copy of the draft Data Protection Policy was made available to all members of staff and to the Board of Management. The suggestions/proposals arising were considered by the Policy Committee in finalizing this policy.

The draft policy was subsequently reviewed and formally ratified by the Board of Management on _____.

Subsequent to BOM ratification, the policy was made available on the shared teacher drive on the school IT network to all teaching staff members. Parents were made aware of the existence and availability of the policy by means of School Newsletter and this policy is also included on the Rush National School website at www.rushnationalschool.ie

The plan will be implemented by the teachers and SNAs supported by the Board of Management from _____.

It will be reviewed every 2 years.

Review Date: _____

Signed: _____

Chairperson of the Board of Management

Date: _____



Rush National School Data Protection Privacy Statement for Parents, Guardians and Pupils 2018 - 2019

Individuals have a number of rights in relation to their personal information – i.e. personal data – and these rights have been enhanced by the General Data Protection Regulation (GDPR). This Data Protection Statement describes how we at Rush National School collect and process personal data, in accordance with the GDPR and the school's legal obligations, generally in relation to the provision of education. Processing is the legal term used to describe various acts including - the collection, recording, organisation, structuring, storage, alteration, use of, retrieval, disclosure or transmission of information.

This statement applies to pupils, parents and guardians. By enrolling your child in and/or by attending Rush National School you acknowledge and agree to the collection and processing of personal information by the school.

For your information this statement outlines:

- Who we are and how to contact us;
- What information we collect, process and retain;
- How information is collected and processed and the purpose and legal basis for so doing;
- Sharing information with third parties;
- Individual legal rights.

WHO WE ARE AND HOW TO CONTACT US

Rush National School is a data controller responsible for personal data - i.e. information relating to an identified or identifiable natural person. Rush National School processes personal data, i.e. the school collects, records, stores, retains and uses personal data. Rush National School will respond to your questions in relation to this Data Protection Statement and our approach to privacy. If you have any questions about this Data Protection Statement, including any request to exercise your legal rights, please contact us at the following email address: dataprotection@rushnationalschool.ie

INFORMATION COLLECTED

Pupil Information

Rush National School may collect and process the following personal information from parents/guardians such as:

- Personal details such as name, address, date of birth, gender, PPS number, nationality, emergency contact information and information in relation to the pupil's family,
- Any special education needs (SEN),
- Any child protection information,
- Academic records, school reports, pupil learning needs, pupil behaviour needs, permission for access to educational reports, individual profile and learning programmes,

- Personal pupil profiles (including whether English is the pupil's first language or if the pupil is exempt from any subjects e.g. Irish or religion),
- Psychological referral/assessment documentation and permission for access to psychological reports,
- Information for the Primary Online Database (POD),
- Information for Special Educational Needs Organiser (SENO),
- Information for TUSLA (the Child and Family Agency) and/or the Health Service Executive (HSE),
- Attendance records and explanatory notes in relation to absences,
- Disciplinary records including notes that may be held by the teacher(s), incident and accident reports, investigations and sanctions if imposed,
- Permission notes in respect of school activities e.g. school tours/trips and outings, extra-curricular activities, (including curricular, RSE/Stay Safe Programme(s)),
- Photographs and recorded images of pupil(s) (including at school events),
- School transport information,
- CCTV footage and other information obtained through electronic means.

Sensitive Personal Information – Pupils

Rush National School may collect and process the following special categories of more sensitive personal information such as:

- Information about pupil's health, medical certificates, medical needs, allergies and consent for administration of medicine,
- Religious belief and confirmation of engagement or not in religious sacraments,
- Membership of the Traveller Community,
- Racial or ethnic origin.

Parent/Guardian Information

Rush National School may collect and process the following personal information from parents/guardians such as:

- Contact details of parent/guardian e.g. name, address, email address, telephone number(s)
- Information regarding legal orders in respect of any family law disputes in respect of guardianship, custody or access,
- Occupation and nationality,
- Number of children, position of pupil(s) in family,
- Consent in respect of medical/other emergencies,
- Consent in respect of school activities e.g. school tours/trips and outings, extra-curricular activities,
- Consent to publish photographs and schoolwork of pupils on school website/print media etc.,
- Records, correspondence or notes arising from interaction with parents/guardians.

PURPOSE & LEGAL BASIS FOR COLLECTING & PROCESSING INFORMATION

Rush National School collects and processes personal information (as listed above) about pupils and parents/guardians for a variety of purposes and relies on a number of legal grounds to do so. Rush National School requires this information to perform our duties and responsibilities and to comply with our legal and statutory obligations. In addition, Rush National School requires this personal information to pursue the legitimate interests of the school and our dealings with relevant third parties (see below).

The legitimate interests upon which we rely is the effective operation and management of Rush National School and managing the education and welfare needs of our pupils. Rush National School processes personal data on the basis of the following lawful purposes:

Legal Obligation

Rush National School collects and processes personal information to comply with our legal and statutory obligations, including, but not limited to, those under the Education Act 1998 (as amended), the Education (Welfare) Act 2000, the Education for Persons with Special Needs (EPSN) Act 2004, the Health Act 1947, the Children First Act 2015, the Child Protection Procedures for Primary and Post-Primary Schools 2017, the Teaching Council Acts 2001-2015 and Safety Health and Welfare at Work legislation.

Legitimate Interests

Rush National School may also process personal information to:

- Enable pupils to develop to their full potential and meet the educational, social, physical, medical and emotional requirements of the pupil,
- Enable parents/guardians to be contacted in the case of emergency, school closures and to inform parents/guardians of their child's educational progress,
- Secure and benefit from the support and services of relevant third parties.

Consent

On occasion, Rush National School processes some of pupils' personal information, with consent, to display on the school's website, on social media platforms strictly moderated by Rush National School, or in the print media. Please note that consent can be withdrawn at any time by writing to the Board of Management of Rush National School.

HOW PERSONAL INFORMATION IS COLLECTED

Pupils

Rush National School collects personal information about pupils through the enrolment process and/or through expressions of interest in relation to enrolment. Additional information is collected from third parties, including former schools and through school activities and general interaction(s), during the course of the pupil's time at Rush National School.

Parents and Guardians

Rush National School collects personal information about parents/guardians through the enrolment process or expressions of interest for enrolment. We collect additional personal information through general interaction during the course of the pupil's time at Rush National School.

INFORMATION AND THIRD PARTIES

Rush National School may receive from, share and/or transfer information to a range of third parties such as the following:

- The Department of Education and Skills,
- TUSLA/the Child and Family Agency,
- The National Council for Special Education,
- National Educational Psychological Service (NEPS),
- Department of Social Protection and/or other state benefit providers,
- An Garda Síochána,
- School Insurance Provider,

- **Third Party Service Providers:** We may share personal information with third party service providers that perform services and functions at our direction and on our behalf such as our accountants, IT service providers including, printers, lawyers and other advisors, and providers of security and administrative services, including data processing/cloud storage service providers e.g. Aladdin Online Schools Management System.

DATA RETENTION

We will only retain personal information for as long as it is necessary to fulfil the purposes the information was collected for, including any legal, accounting or reporting requirements. For more information see the Rush National School Records Retention Schedule.

TRANSFER OF PERSONAL INFORMATION OUTSIDE THE EUROPEAN UNION

Rush National School may transfer the personal information we collect to countries outside the EU. Where there is no adequacy decision by the European Commission in respect of any such country – which means that particular country is deemed not to provide an adequate level of protection for your data – Rush National School will in such circumstances put in place appropriate measures, such as the use of model contractual clauses as approved by the European Commission, to ensure personal information is treated by those third parties in ways that are consistent with respect to EU and Irish Laws on Data Protection.

INDIVIDUAL RIGHTS

Individuals have several rights under GDPR which in certain circumstances are limited and/or constrained. These individual rights include the right – free of charge and subject to any limitations as may apply – to:

1. Request a copy of the personal information held about the individual;
2. Rectify any inaccurate personal data held about the individual;
3. Erase personal information held about the individual;
4. Restrict the processing of individual personal information;
5. Object to the use of individual personal information for our legitimate interests;
6. Receive individual personal information in a structured commonly used and machine-readable format and to have that data transmitted to another data controller.

If you wish to exercise any of these rights please contact us at the school on the following email address: dataprotection@rushnationalschool.ie

Rush National School will endeavour to respond to your request within a month. If we are unable to deal with your request within a month, we may extend this period by a further two months and we will explain why.

You also have the right to lodge a complaint to the office of the Data Protection Commission.

UPDATES

We will update this Data Protection Statement from time to time. Any updates will be made available, and, where appropriate, notified to you.



Rush National School Personal Data Access Request Form

Request for a copy of Personal Data under the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 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 <input type="checkbox"/>	Former Pupil <input type="checkbox"/>	Current Staff Member <input type="checkbox"/>	Former Staff Member: <input type="checkbox"/>	Other* <input type="checkbox"/>
--	---	---	---	---

*** Please indicate connection with the school**

Name of Pupil:	Date of Birth of Pupil:
Insert Years Attended/Worked in the School	From/To:
Insert Year of Leaving:	

Data Access Request

I, [name] wish to make an Access Request for a copy of personal data that Rush National School holds about me/my child. I am making this access request under Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2018.

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

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

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

Signature of Applicant Date:

Please return this form to the relevant address:

The Chairperson of Board of Management
Rush National School
Rush
Co. Dublin



Rush National School Personal Data Rectification/Erasure Form

Request to have Personal Data rectified or erased under the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2018.

Important: Proof of identity (e.g. Official/State photographic identity document such as drivers license, passport) must accompany this form.

Full Name	
Address	
Contact number *	Email addresses *

* The school may need to contact you to discuss your access request

Please tick the box which applies to you:

Pupil	Parent/guardian of Pupil	Former Pupil	Current Staff	Former Staff	Other*
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Age: Class:	Name of Student:	Insert Year of leaving:		Insert Years From/To:	
* Please indicate connection with the school					

I, [insert name] wish to have the data detailed below which Rush National School holds about me/my child rectified / erased (*delete as appropriate*). I am making this access request under **Section 6** of the Data Protection Acts.

Details of the information you believe to be inaccurate and rectification required OR reason why you wish to have data erased:

You must attach relevant documents as proof of correct information e.g. where a date of birth is incorrect, please provide us with a copy of the official State Birth Certificate. Please note that your right to request rectification/deletion is not absolute and may be declined by Rush National School in certain cases. You have the right to complain this refusal to the Office of the Data Protection Commissioner: see www.dataprotection.ie .

Signed Date

Checklist: Have you:

- 1) Completed the Access Request Form in full?
- 2) Included document/s as proof of correct information?
- 3) Signed and dated the Request Form?
- 4) Included a photocopy of official/State photographic identity document (driver's licence, passport, etc.)

Note to school: the school should satisfy itself as to the identity of the individual, and make a note in the school records that identity has been provided but the school should not retain a copy of the identity document.

Please address and return this form to:
Chairperson of the Board of Management,
Rush National School
Rush
Co. Dublin



Rush National School Personal Data Security Breach Code of Practice

Purpose of Code of Practice

This Code of Practice applies to Rush National School as data controller [1]. This Code of Practice will be:

1. available on the school website
2. circulated to all appropriate data processors and incorporated as part of the service-level agreement/data processing agreement between the school and the contracted company and
3. shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the school.

Obligations under Data Protection

The school as data controller and appropriate data processors so contracted are subject to the provisions of the Data Protection Acts 1988 to 2018 and the European Union General Data Protection Regulation 2018 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

The school has prepared a **Data Protection Policy** and monitors the implementation of this policy at regular intervals. The school retains records (both electronic and manual) concerning personal data in line with its **Data Protection Policy** and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

Protocol for action in the event of breach

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

1. The school will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.
2. Where data has been “damaged” (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself (“withholding information”) pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months’ imprisonment on summary conviction.

[1] Unless otherwise indicated, terms used in this Code – such as “personal data”, “sensitive personal data”, “data controller”, “data processor” – have the same meaning as in the Data Protection Acts 1988 to 2018 and the European Union General Data Protection Regulation 2018.

3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude that there is no risk to the data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.
4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.
5. Contact should be immediately made with the data processor responsible for IT support in the school.
6. In addition and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.
7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) have been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 72 hours thereafter), save in the following circumstances:
 - When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) **and**
 - The suspected breach affects no more than 100 data subjects **and**
 - It does not include sensitive personal data or personal data of a financial nature [2].

Where all three criteria are not satisfied, the school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see further details below). Where no notification is made to the Office of the Data Protection Commissioner, the school shall keep a summary record of the incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the incident and an explanation why the school did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

8. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the principal of the school with the practical matters associated with this protocol.
9. The team will, under the direction of the principal, give immediate consideration to informing those affected [3]. At the direction of the principal the team shall:

[2] 'personal data of a financial nature' means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

[3] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows. Where Rush National School receives such a direction from law enforcement agencies, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, Rush National School should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (e.g.. An Garda Síochána), or where this is not possible, Rush National School should write to the relevant law enforcement agency to the

- Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual’s personal data has occurred.
- Where possible and as soon as is feasible, the data subjects (i.e. individuals whom the data is about) should be advised of
 - the nature of the data that has been potentially exposed/compromised;
 - the level of sensitivity of this data and
 - an outline of the steps the school intends to take by way of containment or remediation.
- Individuals should be advised as to whether the school intends to contact other organisations and/or the Office of the Data Protection Commissioner.
- Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal who may, advise the relevant authority e.g. Gardaí, HSE etc.
- Where the data breach has caused the data to be “damaged” (e.g. as a result of hacking), the principal shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
- The principal shall notify the insurance company which the school is insured and advise them that there has been a personal data security breach.

10. Contracted companies operating as data processors: Where an organisation contracted and operating as a data processor on behalf of the school becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school as a matter of urgent priority. In such circumstances, the principal of the school should be contacted directly. This requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.

11. A full review should be undertaken using the template Compliance Checklist and having regard to information ascertained deriving from the experience of the data protection breach. Staff should be apprised of any changes to the Personal Data Security Breach Code of Practice and of upgraded security measures. Staff should receive refresher training where necessary.

Further advice: What may happen arising from a report to the Office of Data Protection Commissioner?

- Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the school shall report the incident to the Office of the Data Protection Commissioner within 72 hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall not involve the communication of personal data.
- The Office of the Data Protection Commissioner will advise the school of whether there is a need for the school to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

effect that “we note your instructions given to us by your officer [insert officer’s name] on XX day of XX at XX pm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach.”

- Should the Office of the Data Protection Commissioner request the school to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:
 - the amount and nature of the personal data that has been compromised
 - the action being taken to secure and/or recover the personal data that has been compromised
 - the action being taken to inform those affected by the incident or reasons for the decision not to do so
 - the action being taken to limit damage or distress to those affected by the incident
 - a chronology of the events leading up to the loss of control of the personal data; and
 - the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.



Rush National School Website Privacy Statement

Rush National School is committed to preserving the privacy of all visitors to our website. This privacy statement relates to our practices in connection with our website and is designed to assist you in understanding how we collect, use and safeguard the personal information you provide to us and to assist you in making informed decisions when using our site and our services. Rush National School fully respects your right to privacy. We will not collect personal information/personal data about you when you visit our website unless you choose to provide that information using the “Contact us” form.

By using this site, you consent to the collection and use of your information under the terms of this privacy statement which is in accordance with the Data Protection Acts 1988 to 2018, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 and the EU General Data Protection Regulation (GDPR). Please read the following privacy statement to understand how we use and protect the information that you choose to provide to us.

What Information do we Collect?

When you visit our website you may provide us with two types of information:

- Personal information you knowingly choose to disclose that is collected on an individual basis, and
- Statistical web site use information collected on an aggregate basis as you and others browse through our website(s)

Email address

When you visit our website you may wish to provide certain information about yourself, such as when you complete our “*Contact Us*” form. **Rush National School** does not collect any personal data about you on this website, apart from the information which you volunteer to send us in the “*Contact Us*” form

Web Site Use Information

Where you visit our website, certain non-personal data is available to us through our internet service provider. This non-personal data is collected on a statistical, aggregate, non-individual basis. This information may include the IP address from which you access our website, the type of internet browser used to access our website, the type of operating system used to access our website, the “top-level” domain name used (ie, .com, .org, etc.), the date and time of your visit to our website and the number of pages you visited on our website

How Do We Use the Information That You Provide to Us?

Any information, which you provide using the “*Contact Us*” form, is not made available to any third parties and is only used by **Rush National School** in line with the purposes for which you provided it (e.g. to contact you and answer any queries which you have raised in the “*Contact Us*” form or to address any other feedback which you send us in the “*Contact Us*” form)

Disclosure to Other People:

We do not disclose, sell or distribute any personal information which you send to us to any third parties. We may pass aggregate information on the usage of our site to third parties, but this will not include information that can be used to identify you. Your personal data may also be anonymised and used for statistical purposes. Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

IP Addresses:

An IP address is a number that is assigned to your computer automatically when you use the internet. When you visit any web page in our website, our servers log your IP address. We may use your IP address to help diagnose problems with our server and to administer our website. Your IP address is also used to help identify you and to gather broad demographic information.

What Are Cookies?

Cookies are a feature of web browser software that allows web servers to recognise the computer used to access a website. Cookies are small pieces of data that are stored by a user's web browser on the user's hard drive

Cookies can remember what information a user accesses on one web page to simplify subsequent interactions with that web site by the same user or to use the information to streamline the web page and to complete commercial transactions over the Internet. Cookies should make your online experience easier and more personalized

Our website uses cookies to keep track of your access to the site. By using our website, you agree that we can place these types of cookies on your device

Your browser will give you the option of preventing websites using cookies, or deleting cookies that have been accepted. Your browser's help service or help manual will show you how this is done. If you do not want your browser to accept cookies, you can "turn off" the cookie acceptance setting on your browser setting. However you must note that this may stop our website from working properly on your device. If you do not change your browser settings to refuse cookies, our website will issue cookies when you visit our website. If you continue to use our website, you agree and consent to our use of cookies on your device

[The school should fully disclose all uses of cookies by their website. The school must obtain full and informed consent of users for the placement of cookies on a user's computer/smartphone etc. This disclosure and explanation should be developed in consultation with the website designer/provider]

Security

We employ security measures to protect your information from access by unauthorised persons and to guard against unlawful processing, accidental loss, destruction and damage and we will do our best to ensure that all records we hold remain secure in line with our obligations under Data Protection Acts 1988 to 2018. We take our security responsibilities seriously, employing appropriate physical and technical measures. We review our security procedures regularly

Retention

We do not retain your personal data for longer than it is necessary for us to comply with the purpose for which you gave it to us. Any personal data which you provide to us using this website will be used in line with the purposes for which you provided it (e.g. to contact you and answer any queries which you have raised in the “**Contact Us**” form or to address any other feedback which you send us in the “**Contact Us**” form) and after this purpose has been completed, we will delete your personal data.

Accessing Your Information

You are entitled to see the information we hold about you. On written request, we supply copies of your personal data, which you may have supplied to us using our website. If you wish to obtain copies of this personal data, you should write to the Board of Management of Rush National School and ask that it provides you with an Access Request Form. Your request will be dealt with as soon as possible and will not take more than a month to process. If you discover that Rush National School holds inaccurate information about you, you can request that we correct/delete that information.

Websites Linked to Our Website

Our website may, from time to time, contain links to and from third party websites. We are not responsible for the practices employed by websites linked to or from our website nor the information or content contained therein. Often links to other websites are provided solely as pointers to information on topics that may be useful to the users of our website

Please remember that when you use a link to go from our website to another website, our Privacy Policy is no longer in effect. Your browsing and interaction on any other website, including websites which have a link on our website, is subject to that website's own rules and policies. Please read over those rules and policies before proceeding

By using our website you consent to our collection and use of your personal information as described in this Privacy Policy. If we change our privacy policies and procedures, we will post those changes on our website to keep you abreast of any developments

Contacting Us

If you are concerned about how your personal data is processed by our website, please bring your concerns to our attention using the contact details below or by email to dataprotection@rushnationalschool.ie.

The Board of Management,
Rush National School
Rush
Co. Dublin

Appendix 6

Aladdin Schools Data Processing Agreement

(A) You, the Board of Management of Rush National School (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.