



# The Red Door School



## Data Protection Policy

**Approved by Board of Management:**

**Reviewed on** 13/6/23

**Next Review Date:** May 2025

**Signed:** \_\_\_\_\_

**Chairperson of Board of Management**



## Data Protection Policy

This policy was formulated by staff and the Board of Management of The Red Door School.

The purpose of this policy is to identify the records required to be retained by the school and to ensure confidentiality and manageable procedures in relation to access to such records by parents and stakeholders.

### Rationale:

A policy on data protection and record keeping is necessary to ensure that the school has proper procedures in place in relation to accountability and transparency.

It is good practice to record pupil progress so as to identify learning needs.

A policy must be put in place in order to ensure our school complies with the following legislation:

- Education Act (Section 9g requiring a school to provide access to records of students over 18/parents)
- Education Welfare Act (requiring a school to report school attendance and transfer of pupils)

### Aims/Objectives:

- To ensure the school complies with legislative requirements;
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies;
- To put in place a proper recording and reporting framework on the educational progress of pupils;
- To establish clear guidelines on making these records available to parents (and pupils over 18);
- To stipulate the length of time records and reports will be retained;

### Guidelines:

The Board of Management of The Red Door School has the function of *data controller* and supervises the application of the Data Protection Acts within the school. The data under the supervision of the Principal comes under the following headings:

#### Students Personal Data:

This data relates to personal details of the students such as name, address, date of birth, gender, home telephone and mobile contact details, ethnic origin, nationality, religious belief, medical details, dietary information and PPSN.



### **Student Records:**

Student records are held by each class teacher, in Storeroom 1, the reception and on Aladdin. Student records contain;-

- Personal details of the student (DOB, address and parent contact details)
- Weekly Data Sheets and, Behavioural Data and Programme Reviews
- Home/School Communication Books (including school communication form and setting events forms filled in daily by staff and parents respectively)
- Psychological Assessments
- Assessment results carried out by professionals to assist teaching and learning (e.g. results of psychiatric reports; occupational therapy reports; speech and language assessments; etc.).
- Assessment records from VB-MAPP, ABLLS and Vineland
- Attendance Records
- Diagnostic Tests Reports
- Individual Education Plans, Individual Pupil Learning Plans, Behaviour Support Plans and records of meetings with the stakeholders regarding these plans
- Portfolios of student work e.g., Evidence folders and achievements on diagnostic tests.

### **Staff Data:**

Name, address, date of birth, contact details, payroll number, PPSN, attendance records, qualifications, school records, references, Garda vetting certificates etc.

### **Administrative Data:**

- Attendance Reports, Roll Book, Registers; Class files; Pupil Profile files; Enrolment applications; birth certificate copy
- Correspondence between parents and teachers.
- Incident Report folder detailing injury and treatment applied.
- Administration of Medicines Indemnity Forms
- Records kept in line with Children First Procedures (Child Protection) manually recorded notes.

### **Access to Records:**

The following will have access where relevant and appropriate to the data listed above where pupils are identified by name:

- Parents/Guardians
- Past Pupils over 18
- Health Service Executive staff
- National Educational Psychological Service



- National Education Welfare Board/Tusla
- Occupational Therapists or Speech Therapists working with pupils
- Designated School Personnel
- Department of Education and Skills (where necessary)

With the exception of child protection-related data which is governed by “Children First Guidelines and Procedures 2011”, data on attendance, (governed by NEWB) and data regarding achievements in literacy and numeracy, (governed by National Strategy for literacy and numeracy), parental authorisation must be provided by parents in the event of data being transferred to outside agencies. Outside agencies requesting access to records must do so in writing. Parents/Guardians of current pupils can make such a request either by phone or in writing. Past pupils and parents of past pupils seeking data must do so in writing.

The end of year report format and its communication to parents are outlined clearly in our school’s Assessment and Records Policy.

### **Data Subject Access Requests (DSAR)**

Staff, students and parents have the right to ask us for a copy of any personal information that we hold. They also have the right to correct and update any personal information that we hold. They may execute any of these rights free of charge and may do so by contacting us:

Phone: + 353 1 6637532

Email: [dataprotection@thereddoorschool.com](mailto:dataprotection@thereddoorschool.com)

When contacting The Red Door to ask about personal information, you may be asked to identify yourself. This is to help protect your information. Once we are satisfied that we have effectively verified your identity, we will respond to the majority of requests without undue delay and within a one month period (i.e. 30 calendar days) of receipt of the request. We will action your request to have your personal information corrected within 10 calendar days. These periods may be extended in exceptional circumstances and we will inform you where the extended period applies to you along with an explanation of the reasons for the extension.

A new provision under GDPR is the data subject’s right to a broader scope of information from the data controller when a data access request is made. The Red Door will provide the following information to the data subject, along with the actual personal data that is being sought under the DSAR:

1. The purposes for processing the data.
2. The categories of personal data concerned.
3. To whom the data has been or will be disclosed.
4. Whether the data has been or will be transferred outside of the EU.



5. The period for which the data will be stored, or the criteria to be used to determine retention periods.
6. The right to make a complaint to the Data Protection Commissioner.
7. The right to request rectification or deletion of the data.
8. Whether the individual has been subject to automated decision making.

#### DSAR Process

##### A. Request

Upon receipt of a DSAR, the Data Protection Officer will log and acknowledge the request. The requestor may be asked to complete a Data Subject Access Request Form to better enable the Company to locate the relevant information.

##### B. Identity verification

The Data Protection Officer needs to check the identity of anyone making a DSAR to ensure information is only given to the person who is entitled to it. If the identity of a DSAR requestor has not already been provided, the person receiving the request will ask the requestor to provide two forms of identification, one of which must be a photo identity and the other confirmation of address. If the requestor is not the data subject, written confirmation that the requestor is authorized to act on behalf of the data subject is required.

##### C. Information for Data Subject Access Request

Upon receipt of the required documents, the person receiving the request will provide the Data Protection Officer with all relevant information in support of the DSAR. Where the Data Protection Officer is reasonably satisfied with the information presented by the person who received the request they will notify the requestor that his/her DSAR will be responded to within 30 calendar days. The 30 day period begins from the date that the request is received. The requestor will be informed by the Data Protection Officer in writing if there will be any deviation from the 30 day timeframe due to other intervening events.

##### D. Review of Information

The Data Protection Officer will collate the relevant and required information as requested in the DSAR. The Data Protection Officer must ensure that the information is reviewed/ received by the imposed deadline to ensure the 30 calendar day timeframe is not breached.

##### E. Response to Access Requests

The Data Protection Officer will provide the finalized response together with the information retrieved and/or a statement that the Company does not hold the information requested, or that an



exemption applies. The Data Protection Officer will ensure that a written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The Red Door will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

#### F. Archiving

After the response has been sent to the requestor, the DSAR will be considered closed and archived by the Data Protection Officer.

#### G. Exemptions

An individual does not have the right to access information recorded about someone else, unless they are an authorized representative.

The Red Door is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

In principle, The Red Door will not normally disclose the following types of information in response to a Data Subject Access Request:

- Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data.
- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and The Red Door will not normally provide a further copy of the same data
- Publicly available information – The Red Door is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by copyright law – The Red Door does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.

#### H. Data Subject Access Request Refusals

There are situations where individuals do not have a right to see information relating to them. For instance:



- If the information is kept only for the purpose of statistics or research, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.
- Requests made for other, non-data protection purposes can be rejected. If the responsible person refuses a Data Subject Access Request on behalf of The Red Door, the reasons for the rejection must be clearly set out in writing. Any individual dissatisfied with the outcome of his/her Data Subject Access Request is entitled to make a request to the Data Protection Officer to review the outcome.

#### **Storage:**

Records are kept for a minimum of 7 years.

- A pupil profile is held for each pupil in a locked cupboard in Principal's Office or Storeroom 1 which have controlled access.
- All completed school roll books and school registers are stored in the Storeroom 1 indefinitely. Digital Roll Books are compiled through the Aladdin Application. Access to these stored files is restricted to authorised personnel only. For computerised records, systems are password protected.

#### **Success Criteria:**

- Compliance with Data Protection Acts
- Reasonably easy access to records
- Manageable storage of records.

#### **Roles and Responsibilities:**

The school staff, under the direction of the principal, will implement and monitor this policy. The principal will ensure records are maintained and stored as directed by the Board of Management.