

# **Data Protection Policy & Procedures**

## **Kildangan NS**

**Data Protection Policy**

**Data Access Request Procedures (Appendix A)**

**Data Breach Code of Practice (Appendix B)**

**Retention of Records Schedule (Appendix C)**

## Kildangan NS Data Protection Policy

### Introduction

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003.

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.

### Data Protection Principles

The school is a *data controller of personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

1. **Obtain and process *Personal Data* fairly:** Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.
2. **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.
3. **Process it only in ways compatible with the purposes for which it was given initially:** Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.
4. **Keep *Personal Data* safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.
5. **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 authorization. If alteration/correction is required, then a note of the fact of such authorization and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

6. **Ensure that it is adequate, relevant and not excessive:** Only the necessary amount of information required to provide an adequate service will be gathered and stored.
7. **Retain it no longer than is necessary for the specified purpose or purposes for which it was given:** As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a 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.
8. **Provide a copy of their *personal data* to any individual, on request:** Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

#### **Definition of Data Protection Terms**

In order to properly understand the school's obligations, there are some key terms which should be understood by all relevant school staff:

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

## Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the principal and board of management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

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

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)
- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs")) such information as the Council may from time to time reasonably request
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of

Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body

- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

### **Relationship to the characteristic spirit of the school**

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

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

### **Personal Data**

The *Personal Data* records held by the school **may** include:

#### **A. Staff records:**

- (a) **Categories of staff data:** As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:
- Name, address and contact details, PPS number
  - Original records of application and appointment to promotion posts
  - Details of approved absences (career breaks, parental leave, study leave etc.)
  - Details of work record (qualifications, classes taught, subjects etc.)
  - Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
  - Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).
- (b) **Purposes:** Staff records are kept for the purposes of:
- the management and administration of school business (now and in the future)
  - to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
  - to facilitate pension payments in the future
  - human resources management
  - recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.

- to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
  - to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
  - and for compliance with legislation relevant to the school.
- (c) **Security & Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. These records are manual records, kept in a manual personal file.

**B. 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 student
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements). See the template "Guidance on Taking and Using Images of Children in Schools"
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory

reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

- (b) **Purposes:** The purposes for keeping student records are:
- to enable each student to develop to their full potential
  - to comply with legislative or administrative requirements
  - to ensure that eligible students can benefit from the relevant additional teaching or financial supports
  - to support the provision of religious instruction
  - to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
  - to meet the educational, social, physical and emotional requirements of the student
  - photographs and recorded images of students are taken to celebrate school achievements, 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 "Guidance for Taking and Using Images of Pupils in Schools" (see template)
  - to ensure that the student meets the school's admission criteria
  - to ensure that students meet the minimum age requirements for their course,
  - to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
  - to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
  - to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers
  - In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.
- (c) **Security & Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Some records are manual records, kept in a personal file, while others are computer records held on a database, which is managed by an outsourced data processing company. This is common practice in the majority of schools in Ireland. 'Aladdin' is the name of the school's current cloud provider; it processes data in accordance with the school's instructions. It is contracted to take appropriate security measures as set down in The Data Protection Acts (Section 2 (1) (d)). All school computer records are maintained with strict security measures including password protection, adequate levels of encryption, NCTE School Firewall and regularly updated anti-virus software.

### **C. Board of Management records:**

- (a) **Categories of board of management data:** These may include:
- Name, address and contact details of each member of the board of management (including former members of the board of management)
  - Records in relation to appointments to the Board

- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.
  -
- (b) **Purposes:** To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.
- (c) **Security & Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Some records are manual records, kept in a personal file, while others are computer records held on an encrypted computer. All school computer records are maintained with strict security measures including password protection, adequate levels of encryption, NCTE School Firewall and regularly updated anti-virus software.

**D. Other records:**

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

**Creditors**

- (a) **Categories of data:** the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
  - address
  - contact details
  - PPS number
  - tax details
  - bank details and
  - amount paid.
- (b) **Purposes:** This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.
- (c) **Security & Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Some records are manual records, kept in a personal file, while others are computer records held on school computers. All school computer records are maintained with strict security measures including password protection, adequate levels of encryption, NCTE School Firewall and regularly updated anti-virus software.

**CCTV images/recordings**

- (a) **Categories:** CCTV is installed in some schools, externally i.e. perimeter walls/fencing 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:** 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. Recording equipment is located in <state location>e.g. the Principal's office or in the reception office of school.
- (d) **Security:** Access to images/recordings is restricted to the principal & deputy principal of the school. Hard disk recordings are retained for 7 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

### **Examination results**

- (a) **Categories:** The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock-examinations results.
- (b) **Purposes:** The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.
- (a) **Security & Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Some records are manual records, kept in a personal file, while others are computer records held on a database, which is managed by an outsourced data processing company. This is common practice in the majority of schools in Ireland. 'Aladdin' is the name of the school's current cloud provider; it processes data in accordance with the school's instructions. It is contracted to take appropriate security measures as set down in The Data Protection Acts (Section 2 (1) (d)). All school computer records are maintained with strict security measures including password protection, adequate levels of encryption, NCTE School Firewall and regularly updated anti-virus software.

### **Other School Policies & Data Protection**

Our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

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

## **Data Subject Rights**

Data in this school will be processed in line with the data subjects' rights.

Data subjects have a right to:

- (a) Request access to any data held about them by a data controller
- (b) Prevent the processing of their data for direct-marketing purposes
- (c) Ask to have inaccurate data amended
- (d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

## **Dealing with Data Access Requests**

### **1. Section 3 access request**

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

### **2. Section 4 access request**

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

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within 40 days
- Fee may apply but cannot exceed €6.35
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

## **Providing Information over the Phone**

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

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

## Sharing student data with the Department of Education

The DES developed an electronic individualised database of primary school children in the school year 2014/2015 in order to monitor the progress of students through the primary system and to aid the development of education policy and forward planning. It is called POD (Primary Online Database). Schools are asked by the DES to provide data including a child's PPS number, name, address, DOB and nationality. Two optional pieces of information about religion and ethnic or cultural background are also sought. These are considered sensitive personal data under Data Protection legislation and require written consent from a parent/guardian for the data to be transferred to the Department. All data on POD is stored on the Revenue Commissioners servers, with the same security protections in place for Revenue records. For more information of POD and the fair processing of student data see DES Circular 0017/2014

### Implementation, Roles & Responsibilities

The Board of Management is the data controller and the Principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

<b>Name</b>	<b>Responsibility</b>
Board of Management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

### Ratification & Communication

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

### Review

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

**Signed:** .....

**Date:** .....

**Chairperson Board of Management, Kildangan NS**

## Appendix A

### Data Access Request Procedures

To make an access request to Kildangan NS, you as a data subject must:

1. Apply in writing requesting access to your data under section 4 Data Protection Acts or, alternatively, request an Access Request Form which will greatly assist the school in processing your access request more quickly. In the case of primary schools, correspondence should be addressed to the Chairperson of the Board of Management.
2. You will be provided with a form which will assist the school in locating all relevant information that is held subject to the exceptions and prohibitions outlined in **Appendix A**. The school reserves the **right to request official proof of identity** (e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification.
3. On receipt of the access request form, a co-ordinator will be appointed to check the validity of your access request and to check that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched).
  - In the case of primary schools, the co-ordinator is the chairperson of the board of management. It may be necessary for the co-ordinator to contact you in the event that further details are required with a view to processing your access request.
4. The co-ordinator will log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.
5. The co-ordinator will ensure that all relevant manual files (held within a "relevant filing system") and computers are checked for the data in respect of which the access request is made.
6. The co-ordinator will ensure that the information is supplied promptly and within the advised timeframes in items 7, 8 and 9 as appropriate.
7. **Where a request is made under Section 3 of the Data Protection Acts**, the following information will be supplied: (i) what the school holds by way of personal information about you (or in the case of a request under section 3 made by a parent/guardian of a student aged under 18 years, then the personal information held about that student) and (ii) a **description** of the data together with details of the purposes for which his/her data is being kept will be provided. Actual copies of your personal files (or the personal files relating to the student) will not be supplied. No personal data can be supplied relating to another individual. A response to your request will be provided within 21 days of receipt of the access request form and no fee will apply.
8. **Where a request is made under Section 4 of the Data Protection Acts**, the following information will be supplied within **40 days and an administration fee of €6.35 will apply**. The individual is entitled to a copy of all personal data, i.e.:
  - A copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts applies, in which case the

individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)

- Be advised of the purpose/s for processing his/her data
  - Be advised of the identity (or the categories) of those to whom the data is disclosed
  - Be advised of the source of the data, unless it is contrary to public interest
  - Where the processing is by automated means (e.g. credit scoring in financial institutions where a computer program makes the “decision” as to whether a loan should be made to an individual based on his/her credit rating), know the logic involved in automated decisions.
9. Where a request is made with respect to **examination results** an increased time limit of **60 days** from the date of the first publication of the results or from the date of the access request, whichever is the later will apply.
10. Before supplying the information requested to you as data subject (or where the access request is made on behalf of a student aged under 18 years, information relating to the student), the co-ordinator will check each item of data to establish:
- If any of the exemptions or restrictions set out under the Data Protection Acts apply, which would result in that item of data not being released, or
  - where the data is “health data”, whether the obligation to consult with the data subject’s medical practitioner applies, or
  - where the data is “social work data”, whether the prohibition on release applies.
11. If data relating to a third party is involved, it will not be disclosed without the consent of that third party or alternatively the data will be anonymised in order to conceal the identity of the third party. Where it is not possible to anonymise the data to ensure that the third party is not identified, then that item of data may not be released.
12. **Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.**
13. The co-ordinator will ensure that the information is provided in an intelligible form (e.g. codes explained) or will provide an explanation.
14. Number the documents supplied.
15. **Have the response “signed-off” by an appropriate person.** In the case of primary schools this is the chairperson of the board of management
16. The school will respond to your access request within the advised timeframes contingent on the type of request made.
17. The school reserves the right to supply personal information to an individual in an electronic format e.g. on tape, USB, CD etc.
18. Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

19. Where you as an individual data subject may seek to rectify incorrect information maintained by the school, please notify the school and a form will be supplied to you for this purpose. You should however note that the right to rectify or delete personal data is not absolute. You have the right to make a complaint to the Data Protection Commissioner about a refusal. Where the school declines to rectify or delete the personal data as you have instructed, the school may propose to supplement your personal record, pursuant to section 6(1)(b) Data Protection Acts.
20. In circumstances where your access request is refused, Kildangan NS will write to you explaining the reasons for the refusal and the administration fee, if provided, will be returned. In such circumstances, you have the right to make a complaint to the Office of the Data Protection Commissioner [www.dataprotection.ie](http://www.dataprotection.ie). Similarly, the administration access fee will be refunded to you if the school/ETB has to rectify, supplement or erase your personal data.
21. **Where requests are made for CCTV footage**, an application must be made in writing and the timeframe for response is within 40 days. All necessary information such as the date, time and location of the recording should be given to the school to assist it in dealing with your request. Where the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data. In providing a copy of personal data, the school may provide the materials in the form of a still/series of still pictures, a tape, disk, USB, with relevant images. Other people's images will be obscured before the data is released. If other people's images cannot be obscured, then the images/recordings may not be released.

**Important note to parents making access requests on behalf of their child:**

Where a parent/guardian makes an access request on behalf of their child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the child is registered on the school's records and will be addressed to the child. The documentation will not be sent to or addressed to the parent/guardian who made the request. Where a parent/guardian is unhappy with this arrangement, the parent/guardian is invited to make an application to court under section 11 of the Guardianship of Infants Act 1964. This provision enables the court (on application by a guardian) to make a direction on any question affecting the welfare of the child. Where a court issues an order stating that a school should make certain information available to a parent/guardian, a copy of the order should be given to the school by the parent/guardian and the school can release the data on foot of the court order.

**Important note to students making access requests:**

Where a student (aged under 18 years) makes an access request, the school may inform the student that:

- (a) Where they make an access request, their parents will be informed that they have done so and
- (b) A complete copy of the access request materials being furnished to the data subject by the school will also be furnished to the student's parent/guardian.

This is provided for in the school's Data Protection Policy. The right of access under the Data Protection Acts is the right of the data subject. However, there may be some data held by the school which may be of a sensitive nature and the school will have regard to the following guidance issued by the Office of the Data Protection Commissioner in relation to releasing such data:

- A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- A student aged from **twelve up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that:
  - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
  - If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent before releasing the data to the student
  - If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.
- In the case of students **under the age of twelve**, an access request may be made by their parent or guardian on the student's behalf. However, the school must note that the right of access is a right of the data subject themselves (i.e. it is the right of the student). Therefore, access documentation should be addressed to the child at his/her address which is registered with the school as being his/her home address. **It should not be addressed or sent to the parent who made the request.** For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.

**Important note to individuals making an access request:**

On making an access request, any individual (subject to the restrictions outlined above) about whom a school keeps Personal Data, is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing his/her data
- know the identity (or the categories) of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest

**Implementation & Review**

The Data Access Request Procedures of Kildangan NS will be implemented from May 2015. They will be reviewed and evaluated when necessary by the Board of Management, particularly if affected by changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, Department of Education and Skills, national management bodies, legislation and feedback from parents/guardians, students, staff and others.

The date from which these procedures apply is the date of adoption by the Board of Management. Implementation of the policy will be monitored by the Principal.

## Appendix B

### Kildangan NS Data Breach Code of Practice

#### Purpose of the Code of Practice

This Code of Practice was formulated by Kildangan NS, in line with its Data Protection Policy drafted and ratified by the Board of Management, in consultation with staff and the school's Parents Association in April 2015. This code of practice applies to the school as the school is the *data controller*[1].

#### Obligations under Data Protection

The school as data controller and appropriate data processors contracted by the school, are subject to the provisions of the Data Protection Acts, 1988 and 2003 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 prioritize 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 a breach:

In circumstances where an incident gives rise to a risk of unauthorized 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.
3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorized 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.

---

[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 and 2003.



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) has 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 2 working days 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 unauthorized 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. The team will, under the direction of the principal, give immediate consideration to informing those affected[3].
9. At the direction of the principal the team shall:
  - Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorized 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

---

[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 Kildangan NS 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, Kildangan NS should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Síochána), or where this is not possible, the school should write to the relevant law enforcement agency to the effect that "we note your instructions given to us by your officer [insert officer's name] on XX day of XX at XXpm 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."

- 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 organizations 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 organization contracted and operating as a *data processor* on behalf of the school becomes aware of a risk to personal/sensitive personal data, the organization 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 when necessary 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 **two working days** 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.
- 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.

## Appendix C

### Retention of Records

Schools as *data controllers* must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It may also be anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, Kildangan NS has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary. All records will be periodically reviewed in light of experience and any legal or other relevant indications.

**IMPORTANT:** In all cases, schools should be aware that where proceedings have been initiated, are in progress, or are reasonably foreseeable (although have not yet been taken against the school/board of management/an officer or employee of the school (which may include a volunteer)), all records relating to the individuals and incidents concerned should be preserved and should under no circumstances be deleted, destroyed or purged. The records may be of great assistance to the school in defending claims made in later years.

**WARNING:** In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim and the Statute of Limitations may be different in every case. In all cases where reference is made to “18 years” being the date upon which the relevant period set out in the Statute of Limitations commences for the purposes of litigation, the school must be aware that in some situations (such as the case of a student with special educational needs, or where the claim relates to child sexual abuse, or where the student has not become aware of the damage which they have suffered, and in some other circumstances), the Statute of Limitations **may not begin to run when the student reaches 18 years of age and specific legal advice should be sought by schools on a case-by-case basis.** In all cases where retention periods have been recommended with reference to the relevant statutory period in which an individual can make a claim, these time-frames may not apply where there has been misrepresentation, deception or fraud on the part of the respondent/defendant. In such a circumstance, the school should be aware that the claim could arise many years after the incident complained of and the courts/tribunals/employment fora may not consider the complainant to be “out of time” to make their claim.

**Please see Retention of Records Schedule attached**

