DATA PROTECTION POLICY

DATA PROTECTION POLICY

Introduction:
The purpose of the 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, staff and other stake holders.

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 to ensure a school complies with legislation such as;

    - Education Act 1998
    - Education Welfare Act 2000
    - Data Protection Act 2003
    - Freedom of Information Act 1997
    - The National Strategy to improve Literacy and Numeracy among Children and Young People 2011 – 2020

Details of arrangements in place to ensure compliance with the eight rules of data protection

The policy will be implemented so as to ensure that all personal data records held by the school are obtained, processed, used and retained in accordance with the following eight rules of data protection (based on the Data Protection Acts):

1. Obtain and process information fairly
2. Keep it only for specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to that individual on request.

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 years of age.

- To stipulate the length of time records and reports will be retained

Guidelines:
The Principal assumes the function of data controller and supervises the application of the Data Protection Act within the school. The data under the control of the Principal comes under the following headings.

A. <u>Personal Data:</u>
This data relates to personal details of the students such as name, address, date of birth, gender, family status, parents' place of employment, ethnic origin, nationality, religious belief, medical details, dietary information, PPSN, home telephone and mobile contact details. It also includes the names of students' parents/guardians. This information is included in the School Enrolment Form. These forms are kept in the secretary's/principal's Office. Information such as name, address, contact numbers and registration numbers on pupils are stored in both hard and soft copy format.

Student Records:

Student records outlined below are held by each class/SET teacher and/or in the principal's Office. Such student records contain;-

- Personal details of the student
- School report cards
- Attendance Records
- Records of students who have been granted exemption for the study of Irish.
- Teacher-designed tests. Each class teacher designs his/her own tests.
- Individual Education Plans, Individual Pupil Learning Profiles and records of meetings with the stakeholders regarding these plans
- Special Education Data such as records of permissions/refusals to allow children access to SET services in the school
- Screening Tests e.g. M.I.S.T., N.R.I.T., Dyslexia Screening Tests etc.
- Portfolios of student work e.g. Projects/Art and achievements on diagnostic tests.

  Databiz solutions records are also stored on the main school computer housed in the secretary's office and on the DES esinet portal which encompasses Primary online database POD.

The following records are stored securely in the Principal's Office

- 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.).
- Standardised Test Results
- Child Protection concerns and HSE referrals
- Minutes of HSE Child Protection Conferences.

B. **Administrative Data:**

- Attendance Reports, Roll Book, Registers; Class files; Pupil Profile files; Enrolment applications; baptismal certificate copy (where applicable); birth certificate copy, passport copy if necessary.
- Correspondence between parents and teachers.
- Accident Report Book detailing injury and treatment applied
- Administration of Medicines Indemnity Forms
- Late arrivals/early leaving records
- Pupil behaviour records and Records of allegations/ incidents of bullying and alleged bullying; (manually recorded notes), (kept in Principal's Office)
- Records kept in line with Children First Procedures (Child Protection) (kept in Principal's Office)

Board of Management records*:* These include:

- Name, address and contact details of each member 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.
- Minutes, reports and correspondence relating to the Board of Management are kept in the Principal's office. Child Protection matters reported to the Board will not identify a pupil by name except in exceptional circumstances.

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
- Occupational Therapists or Speech Therapists working with pupils
- Designated School Personnel
- Department of Education and Skills (where necessary)
- First and Second level schools (where relevant)
- School Board of Management

With the exception of child protection-related data which is governed by "Children's 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) and POD (governed by DES) 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 in writing. Past pupils and parents of past pupils seeking data must do so in writing.

The Annual School Report format and its communication to parents are outlined clearly in our schools Assessment Policy. A standardised school report form is used, which is issued by hand in June to all parents which includes results of standardised testing of pupils from 1st to 6th classes.

C. <u>Staff Data</u>

Staff records include name, address, contact details, payroll number, PPSN, qualifications, records of interview procedures, results of interview process, Interview board recommendations to BOM, BOM recommendations to patron, contracts, pension details, references, curriculum vitae, job applications, attendance records, Teaching Council registration, Garda Clearance, Statutory Declaration, where necessary, Medical Fitness to Teach. Access is restricted to the Principal and Secretary. Records are destroyed by way of shredding when no longer required.

These records are kept in the Principal's office. Attendance details are recorded on the OLCS system, are password protected and are accessed by the Secretary, the Principal , the Deputy Principal and the Chairperson of the Board of Management if necessary.

D. Students' Attendance Records:

Pupils' attendance will be recorded and stored on the Databiz software administration system. This system is password protected and is accessed by the class teacher, secretary and the principal.Teachers can access their own class records in any given year. These class records are password protected.

E. <u>Student Records:</u>

Student records maintained under the Data Protection Policy will include:

1. ***School Reports***. An annual progress report is issued to each child's parent/guardian at the end of the school year. A copy of this report is available on request to a parent who resides at a different address. These reports are securely stored on the Databiz software.
2. ***Psychological Assessments***. Reports issued following psychological assessment are securely stored in the Principal's Office. Reports issued following other assessments such as Occupational Therapy, Speech & Language, Medical etc are also stored in the Principal's Office.
3. ***Standardised Test Results***. Standardised Tests in English and Mathematics are administered in May to all classes from First Class to Sixth Class. Class Record Sheets are securely stored by the Class Teacher and SET Teacher. The Principal will also retain a copy of class record sheets.

Standardised Test results are included in the Annual Summer Report to be completed at the end of the school year and stored in the Secretary's Office. Test Booklets are stored cumulatively by Class Teachers until pupil leaves school after which they are shredded.

4. ***Screening Tests***. The MIST (Middle Infant Screening Test) Assessment is administered to all Senior Infant children in February/March of each year. Class record sheets are securely stored by the class teacher and the SET teacher.
5. ***Teacher – designed tests***. Results of teacher designed tests are securely stored by the teacher.
6. ***Diagnostic Test Reports***. Diagnostic tests are administered by the Support Teachers. Results from these assessments are securely stored by the relevant teachers and details may also included in records kept by the Principal.
7. ***Special Educational Needs***. Classroom Support Plans, School Support Plans and School Support Plus Plans will be completed by relevant teachers for children with Special Educational Needs. Copies will be securely stored by teachers, relevant Support Teachers and a copy included in the Principal's records.
8. ***Learning Support/Resource Data*** such as records of consent/refusal to allow diagnostic testing or access to Support Teacher services in the school. These records are securely stored on the Databiz system, in the SET rooms and in the Principal's office.
9. ***Class Records.*** Class records are updated regularly. Class record sheets are stored securely in class folders in teachers' classrooms.
10. ***Portfolios*** of student work e.g. Art, Written work are stored securely by the Class Teacher.
11. ***Attendance Records.*** Rolls are maintained by the Class Teacher. Attendance and punctuality details are included in the school's computerized data management system. Computerised records (databiz) are securely stored in a password protected folder.
12. ***Record of child's breaches of Code of Behaviour.*** Incidents of misbehaviour in the playground are recorded in notebooks and stored in the relevant bags in the seomra foirne. Each Class Teacher keeps a record of classroom incidents. The Principal maintains a record of incidents brought to her attention. Incidents of serious misbehaviour resulting in a suspension are retained by the Principal.
13. ***Records of serious injuries/accidents.*** The accident Report Folder is stored in the seomra foirne with each year's moved to the Principal's office. The teacher in charge records details of accidents and injuries sustained and action taken.
14. ***Indemnity Form for Administration of Medicine.*** These forms are retained in the Principal's office.
15. ***Certificates of Exemption from the Study of Irish.*** Copies of certificates are securely stored by the Principal.

Storage:

Records are stored until pupils reach the age of 21 years. In the case of children with Special Educational Needs, records are stored until they reach the age of 24 years.

All completed school Roll Books, Registers and Leabhar Tinrimh are stored in the same location together with Accident Report Books and Incident/Bullying Report Books.

Access to these stored files is restricted to authorised personnel only. For computerised records, systems are password protected.

Access to Pupil Records:
A parent may apply for access to their records until the child reaches the age of 18 years. A past pupil may apply for access to their own records from the age of 18 years to 21 years.

A written application will be required, accompanied by a form of identification and Birth Certificate. Records will be provided within 21 days.

Transfer of Student Records:
A parental authorisation form must be completed by parents in the event of data being transferred to outside agencies, including other Primary Schools and Secondary Schools. When a pupil transfers to another Primary School the new school will notify the original school and the original school will transfer records of attendance and educational progress to them. A standard School Report Form is used for this purpose.

CCTV data usage:
CCTV cameras are in operation at the following points in the school;

1. 1 camera in Junior Playground monitoring the playground activity area.

Use of CCTV images;
The use of this CCTV system is intended primarily to ensure the security of the school equipment. The CCTV system may be used to capture images of intruders or of individuals damaging property or removing goods without authorisation.

A sign informing data subjects that the CCTV system is in operation will be displayed at the entrance to the school. Images captured by the CCTV system will be retained on the monitor for a month. In exceptional circumstances images may be retained where an investigation by An Garda Síochána is ongoing or where such images are the subject of court proceedings.

If the Gardaí want CCTV images for a specific investigation, the data controller will satisfy herself that there is a genuine investigation underway. A phone call to the requesting Garda's station will be sufficient, provided that the data controller speaks to a member in the District Office, the station sergeant or a higher ranking officer, as all may be assumed to be acting with the authority of a District/Divisional officer in confirming that an investigation is authorised.

Any person whose image has been recorded has a right to be given a copy of the information recorded. To exercise that right, a person must make an application in writing. A data controller will charge up to €6.35 for responding to such a request and will respond within 40 days.

Practically, a person must provide necessary information to the data controller, such as the date, time and location of the recording. If 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 giving a person a copy of his/her data, the data controller may provide a still/series of still pictures, a tape or a disk with relevant images. However, other people's images will be obscured before the data are released.

Success Criteria:

- Compliance with Data Protection Act and Statute of Limitations Act
- Easy access to records
- Framework in place for ease of compilation and reporting
- 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 that records are maintained and securely stored.

Review/Ratification/Communication:
This policy was ratified by the Board of Management on 19th October 2017. It will be subject to review as the need arises.

_____, Date: _____
Rev Brian Early

References:

1. *Solas (CPSMA) May-June 2001*
2. *Education Act 1998*
3. *Education Welfare Act 2000*
4. *Data Protection Act 2003*
5. *Freedom of Information Act 1997*
6. *Literacy and Numeracy Strategy 2011*

Data Protection and CCTV

The use of CCTV systems has greatly expanded in recent years. So has the sophistication of such systems. Systems now on the market have the capacity to recognise faces. They may also be capable of recording both images and sounds.

The expanded use of CCTV systems has society-wide implications. Unless such systems are used with proper care and consideration, they can give rise to concern that the individual's "private space" is being unreasonably eroded.

Recognisable images captured by CCTV systems are personal data". They are therefore subject to the provisions of the Data Protection Acts.

A data controller needs to be able to justify the obtaining and use of personal data by means of a CCTV system. A system used to control the perimeter of a building for security purposes will usually be easy to justify. The use of CCTV systems in other circumstances – for example, to constantly monitor employees, customers or students – can be more difficult to justify and could involve a breach of the Data Protection Acts.

Proportionality – is a CCTV system justified?

Section 2(1)(c)(iii) of the Acts require that data are "adequate, relevant and not excessive" for the purpose for which they are collected. This means that an organisation must be able to demonstrate that the serious step involved in installing a system that collects personal data on a continuous basis is justified. Before proceeding with such a system, it should also be certain that it can meet its obligations to provide data subjects, on request, with copies of images captured by the system.

Proportionality – what will the system be used for?

If a data controller is satisfied that it can justify installing a CCTV system, it must consider what it will be used for and if these uses are reasonable in the circumstances.

Security of premises or other property is probably the most common use of a CCTV system. Such a system will typically be intended to capture images of intruders or of individuals damaging property or removing goods without authorisation. Such uses are more likely to meet the test of proportionality.

Other uses may fail the test of proportionality. For example, using a CCTV system to constantly monitor employees is highly intrusive and would need to be justified by reference to special circumstances. If the monitoring is for health and safety reasons, a data controller would need to demonstrate that the installation of CCTV was proportionate in addressing health and safety issues that had arisen prior to the installation of the system.

Proportionality – what images will be captured?

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Toilets and rest rooms are an obvious example.

To justify use in such an area, a data controller would have to demonstrate that a pattern of security breaches had occurred in the area prior to the installation of the system such as would warrant constant electronic surveillance. Where such use can be justified, the CCTV cameras should never be capable of capturing images from cubicles or urinal areas.

Cameras placed so as to record external areas should be positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

Transparency

Section 2D of the Acts requires that certain essential information is supplied to a data subject before any personal data are recorded. This information includes:

the identity of the data controller;
the purposes for which data are processed;
any third parties to whom the data may be supplied.

This can usually be achieved by placing easily- read and well-lit signs in prominent positions. A sign at all entrances will normally suffice.

If the identity of the data controller and the usual purpose for processing – security - is obvious, all that need be placed on the sign is a statement that CCTV is in operation as well as a contact (such as a phone number) for persons wishing to discuss this processing. This contact can be for either the security company operating the cameras or the owner of the premises.

If the purpose or purposes is not obvious, there is a duty on the data controller to make this clear. A CCTV camera in a premises is often assumed to be used for security purposes. Use for monitoring staff performance or conduct is not an obvious purpose and staff must be informed before any data are recorded for this purpose. Similarly, if the purpose of CCTV is also for health and safety reasons, this should be clearly stated and made known.

Storage and retention.

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which they were obtained. A data controller needs to be able to justify this retention period. For a normal security system, it would be difficult to justify retention beyond a month, except where the images identify an issue – such as a break-in or theft - and is retained specifically in the context of an investigation of that issue.

The storage medium should be stored in a secure environment with a log of access kept. Access should be restricted to authorised personnel.

Supply of CCTV Images to An Garda Síochána

If the Gardaí want CCTV images for a specific investigation, it is up to the data controller to satisfy himself that there is a genuine investigation underway. For practical purposes, a phone call to the requesting Garda's station may be sufficient, provided that you speak to a member in the District Office, the station sergeant or a higher ranking officer, as all may be assumed to be acting with the authority of a District/Divisional officer in confirming that an investigation is authorised.

Access Requests

Any person whose image has been recorded has a right to be given a copy of the information recorded. To exercise that right, a person must make an application in writing. A data controller may charge up to €6.35 for responding to such a request and must respond within 40 days.

Practically, a person should provide necessary information to a data controller, such as the date, time and location of the recording. If 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 giving a person a copy of his/her data, the data controller may provide a still/series of still pictures, a tape or a disk with relevant images. However, other people's images should be obscured before the data are released.

Covert surveillance.

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána.

Covert surveillance must be focused and of short duration. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.

If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy.

Responsibilities of security companies.

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors". As data processors, they operate under the instruction of data controllers (their clients). Sections 2(2) and 2C of the Data Protection Acts place a number of obligations on data processors.

These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.

Staff of the security company must be made aware of their obligations relating to the security of data.

Clients of the security company should have a contract in place which details what the security company may do with the data; what security standards should be in place and what verification procedures may apply.

Furthermore, section 16 of the Data Protection Acts 1988 & 2003 requires that certain data processors must have an entry in the public register maintained by the Data Protection Commissioner. For further information, please refer to our Guidance notes on Registration. Those parties who are required to be registered and process data whilst not registered are committing a criminal offence and may face prosecution by this office. (This provision may only apply where the data controller can identify the persons whose images are captured.)

Domestic use of CCTV systems.

The processing of personal data kept by an individual and concerned solely with the management of his/her personal, family or household affairs or kept by an individual for recreational purposes is exempt from the provisions of the Acts. This exemption would generally apply to the use of CCTVs in a domestic environment. However, the exemption may not apply if the occupant works from home. [Where the exemption does apply, a person who objects to the use of a CCTV system – for example, a neighbour who objects to images of her/his property being recorded – may be able to take a civil legal action based on the Constitutional and Common Law right to privacy.]

Community CCTV Schemes

Comprehensive guidelines in relation to Community based CCTV schemes are available on the Department of Justice Website at the following link: http://www.justice.ie/en/JELR/Pages/Community_CCTV

Some Case Studies relevant to this topic:
The following Case Studies, which have appeared in Annual reports of the Data Protection Commissioner over recent years, may be of some interest. Click on the Case Study details to see the full text.

CASE STUDY 3/07 – Inappropriate use of CCTV footage by Leisure Club
CASE STUDY 6/07 – Data Controller breaches Data Protection Law in regard to covert use of CCTV footage
CASE STUDY 11/06 – Failure to comply with an Access Request for CCTV footage
CASE STUDY 8/05 - CCTV cameras on the Luas line