USE OF DATA POLICY

Circular Letter 0047/2010

To the Boards of Management of Post-Primary Schools and the Chief Executive Officers of Vocational Education Committees

Fair Processing Notice to explain how the personal data of students enrolled at post primary schools as at 30th September and which is returned by post-primary schools to the Department of Education and Skills each year, is processed fairly and in compliance with the Data Protection Acts 1988 to 2003.

Each year, each recognised post primary school makes a return to the Department of Education and Skills, the data from which allow the Department of Education and Skills calculate the teaching posts and core funding to be allocated to each recognised post primary school, for the following school year.

These returns are made in accordance with ***The Rules and Programme for Secondary Schools***[1] via a process called the *Annual Post-Primary School October Return/Examination Entries,* or more familiarly known as the October Returns. In making their respective returns to the Department, post primary schools transfer personal data and personal sensitive data on each of their enrolled students. The only purpose some post primary schools may collect some of these data is to meet the data requirements for their October Return to the Department.

Schools are data controllers[2] for the data they collect for their own purposes including collecting and transferring data to avail of the funding and services provided by the Department. The Department has reminded schools of their own obligations under the Data Protection Acts and has made information on this available through the Department's website www.education.ie to assist schools in this regard.

[1] A "**secondary school**" means a school which is recognised by the Minister as providing instruction in an approved curriculum and which complies with the *Rules and Programme for Secondary Schools*. School in this category include secondary voluntary, vocational and community & comprehensive post-primary schools.

[2] **Data controller** means a person who, either alone or with others, controls the contents and uses of personal data

Post primary schools return their data electronically through the secure *esinet* network system. The data received by the Department from post primary schools through the October Returns is stored in a secure database, called the Post Primary Pupil Database. It is Departmental policy that only a small number of staff who have a requirement to view these personal data for work purposes can gain access to these data.

Upon receipt, the Principal Officer, Parents' Learners' and Database Section of Schools' Division becomes the data controller for these data. The Department of Education and Skills is committed to:

- abiding by the Data Protection Acts 1988 to 2003,
- respecting peoples' rights to confidentiality and for privacy,
- keeping up to date all data about recognised students stored on its database.

Allocating resources to post primary schools to meet the individual needs of each student requires the Department collecting and validating data on each student enrolled in a recognised post primary school. To meet the Department's business needs in this regard, the Department shares a limited amount of each student's personal data, including a child's PPS number with the Department of Social Protection. The legal basis for this sharing of data is set out in Social Welfare Acts[3]. The primary reason for this is to assist the Department validate that each student returned by post primary schools is a recognised student, in accordance with *The Rules and Programme for Secondary Schools.*

The Department does share some of the personal data with other State bodies. These are:

- Data on students enrolled in exam years with the State Examinations Commission to assist its planning for state examinations.
- Central Statistics Office, under the Statistics Acts to assist with the compilation of national statistics.
- Data on 15 years old students, excluding their PPS number to the Educational Research Centre to meet its research requirements which includes some of Ireland's international research requirements. This Centre subsequently liaises with post primary schools in respect of further data it may require on individual students to assist their research requirements.

The Department has a data user agreement with each of these bodies, which includes the purpose for which the body requires the data, its storage, security and retention. Details of existing data user agreements are available on the Department's website at www.education.ie (and search for October Returns).

[3] **Section 266** of the **Social Welfare Consolidation Act 2005** states that "Notwithstanding anything contained in any other enactment, a specified body may share any information that may be prescribed with (a) the Minister for Education and Science, where the Minister requires the information for the purposes of enabling him or her to provide education in accordance with **section 6(b)** of **the Education Act 1998"** A recognised school within the meaning of section 2 of the Education Act has been designated a specific body for these purposes. Regulation 189 of the **Social Welfare(Consolidated Claims, Payments and Control) Regulations 2007 (S.I. No. 142 of 2007)** lists the prescribed information for the purposes of section 266 in relation to a pupil that may be shared.

The Department uses these data stored in Post Primary Pupil Database for planning, policy and statistical purposes. However it does not use individual data for these purposes, but rather aggregates these data to meet its business needs in these areas. A small number of the data returned by schools as part of the October Return are required for these purposes only.

The Department retains personal data on each student up to their 25th birthday and subject to review thereafter. Since 1991, the Department has retained all individual data on students returned by post primary schools via their October Return. The purpose of this retention policy serves to trace student retention, is important for research and policy formation as well as being an important statistical indicator nationally and internationally. Again aggregate and not individual data is used for these purposes.

Individual records are also retained to meet individual requests from former students which may require it for employment or other purposes. The Post Primary Pupil Database is currently the only national archive of student enrolment at post primary schools.

The Department is continually reviewing its retention policy for student data in consultation with the Office of the Data Protection Commissioner and will update its retention policy from time to time. Any amendments will be available on the Department's website, www.education.ie

Jointly Meeting the Data Protection Requirements for October Returns

In previous years, school authorities signed a declaration that they had fulfilled their data protection obligations in relation to the collection and transfer of the data for their school's October Returns. The Department had available on its website the relevant data protection information for parents in relation to its use and purpose of the data returned by schools through the October Return process.

This year the Department has consulted with the management bodies for post primary schools and have jointly agreed the benefits of adopting a common template and approach to gaining the consent of enrolled students aged over 18 years or from the parents /guardians of younger students.

The Department has met with officials from the Data Protection Commission Office to inform the approach to be taken. In summary and in relation to the October Returns, there are two distinct categories of consent required and approaches to be adopted as follows:

- personal data such as name, address, PPS number, subjects being studied etc. It is appropriate for these data fields, to inform parents/guardians and students (over 18 years) that the school and Department do collect these data, setting out the purpose, storage, what other bodies it is shared with and its retention.
- sensitive personal data refers, in the context of the October Returns, to seeking a person's medical card eligibility and membership to the Travelling Community. In relation to these fields the express written consent of the parents/guardians or students (over 18 years) is required, before returning these individualised data to the Department.

The Department requires data on medical card eligibility for statistical and policy purposes and it may inform indicators for the classification of DEIS schools. Data on membership to the travelling community is required for the purpose of allocating appropriate resources to schools to meet the individual needs of these children. Post primary school authorities are required to gain the written consent from the relevant parents/guardians and students before returning individualised data on these two data fields. Schools do not need to return the written consent with the October Returns but should retain it for any inspection by either the Department or the Data Protection Commissioner.

In both categories parents/guardians and students (over 18 years) have the right to object to the processing of their child's (or their own) personal data, to block certain uses of the data and also in the unlikely event that they identify any errors in these data held about their child (or themselves), they have the right to correct such errors.

To assist schools and the Department comply with their respective data protection requirements for the annual October returns, post primary schools are asked to refer to the attached template. This is a notice to parents, guardians and students aged 18 years and over, on how the personal data of students enrolled at post primary schools as at 30th September, is returned to the Department of Education and Skills, to primarily secure teaching posts and core funding; and how these data are processed fairly and in compliance with the Data Protection Acts 1988 to 2003.

Schools are empowered to either circulate the attached notice to parents or to amend, as necessary, their current arrangements for seeking consent for the October Return by reference to this circular and template.

Brian Brogan
Principal Officer
Schools' Division
August 2010

Notice to Parents, Guardians and Students aged 18 years and over, on how the personal data of students enrolled at this post primary school as at 30th September, is returned to the Department of Education and Skills, to primarily secure teaching posts and core funding; and how these data are processed fairly and in compliance with the Data Protection Acts 1988 to 2003.

Introduction

For the Department of Education and Skills to be able to allocate teaching staff and core funding to this post primary school to meet your child's educational needs, the Department must collect individual and personal data on each student enrolled in each recognised post primary school, at 30th September each year.

This notice sets out the details of the personal data being collected, its purpose, what other bodies these data are shared with and why; how the Department securely stores these data and the Department's retention of these data.

Purposes of Collecting Individual Student Data

Teaching posts and core funding are allocated to post primary schools by the Department of Education and Skills each year, based on the number of *recognised* students enrolled in each post primary school, as at 30th September in the previous year.

The Department has detailed in ***The Rules and Programme for Secondary Schools*** the criteria for a *recognised student in post primary schools*. While the full set of rules is available on the Department's website, www.education.ie, examples include:

- a student meeting the minimum age requirement for their course and that they are following an approved course, e.g. Junior Certificate, and
- given Irish is a compulsory subject for all post primary students, those students not studying Irish must have been granted an exemption from Irish by the school authorities, in accordance with criteria for granting such exemptions.

Hence for each post primary school to have the appropriate levels of teaching posts and core funding to meet your child's educational needs, each post primary school is required to transfer individualised date on each student enrolled in our school to the Department, as part of what is commonly referred to as the school's October Return. Much of these data the school would have to assist its management of the school, but some data schools collect specifically for the purpose of making this return.

The core funding allocated to schools includes provision of English Language Support to those students with limited or no knowledge of English and additional resources to meet the educational needs of children who are members of the Travelling Community.

The Department has to meet many national and international statistical, policy and research requirements. The Department does not use individual data from these returns for these functions. However the Department aggregates the individual data for these purposes as well as assisting its wider planning functions.

How is the October Return Made and Where and How are the Data Stored?
Post primary schools return their data electronically through the secure *esinet* network system. The data received by the Department from post primary schools through the October Returns is stored by the Department in its secure database, called the Post Primary Pupil Database. It is Departmental policy that only a small number of staff who have a requirement to view these personal data for work purposes can gain access to these data.

Upon receipt, the Principal Officer, Parents' Learners' and Database Section of Schools' Division becomes the data controller for these data. The Department of Education and Skills is committed to

- abiding by the Data Protection Acts 1988 to 2003,
- respecting peoples' rights to confidentiality and for privacy, and
- keeping up to date all data about recognised students stored on its database.

What personal data is collected?
A list of the specific data collected on each student and the purpose for which each item is collected is attached for your information.

What Bodies Does the Department Share Some of the Individual Data With?

As it is necessary to return individualised data to the Department, the Department uses each student's Personal Public Service Number as a unique identifier. As part of validating that each student returned by post primary schools is a *recognised* student, the Department transfers a limited amount of each individual student's personal data to the Department of Social Protection. This includes each child's PPS number. The legal basis for this sharing of data is set out in Social Welfare Acts.

Sharing a limited amount of the personal data with the Department of Social Protection is also important to:

- identify students that have similar details. For example, a student can only be enrolled in one school as at 30th September,
- in cases where a child's PPSN number is not available, their individual identity can be determined from the student personal data together with her/his mother's maiden name,
- identify the movement of students between schools over their time within the education system while allowing their course data from different schools to be accessed for recognition purposes.

Hence a student's PPS number provided through the October Returns is to provide a unique identifier for each student and as part of validating that each student is a *recognised* student.

The Department does share some of the personal data with other State bodies. These are:

- data on students enrolled in exam years with the State Examinations Commission to assist its planning for state examinations,
- Central Statistics Office, under the Statistics Acts to assist with the compilation of national statistics, and
- data on 15 years old students, excluding their PPS number to the Educational Research Centre to meet its research requirements which includes some of Ireland's international research requirements. This Centre subsequently liaises with post primary schools in respect of further data it may require on individual students to assist their research requirements.

The Department has a data user agreement with each of these bodies, which includes the purpose for which the body requires these data, its storage, security and retention. Details of existing data user agreements are available on the Department's website at www.education.ie (and search for October Returns).

Retention of student data

The Department retains personal data on each student up to their 25th birthday and subject to review thereafter. Since 1991, the Department has retained all individual data on students returned by post primary schools via their October Return. The purpose of this retention policy serves to trace student retention, is important for research and policy formation as well as being an important statistical indicator nationally and internationally. Again aggregate and not individual data is used for these purposes.

Individual records are also retained to meet individual requests from former students which may require it for employment or other purposes. The Post Primary Pupil Database is currently the only national archive of student enrolment at post primary schools.

The Department is continually reviewing its retention policy for student data in consultation with the Office of the Data Protection Commissioner and will update its retention policy from time to time. Any amendments will be available on the Department's website, www.education.ie

Accessing Personal Information

As part of the fair processing of these data for the October Returns by and between post primary schools and the Department of Education and Skills, post primary schools seek the consent from parents or guardians of children under 18 years and directly from students over 18 years of age.

This notice informs parents and students of the data collected through the October Returns and its uses. No written consent is required except in the cases of what is termed *sensitive personal data*. In the case of the October Returns the Data Protection Commissioner's Office has advised that two data fields fall under this category, namely 1st year student's medical card eligibility and membership of any student to the Travelling Community.

Post primary school authorities are required to gain the written consent from the relevant parents/guardians and students before returning individualised data on these two data fields. If either of these data fields apply to your child, or if you are an enrolled student and aged over 18 years and these data fields apply to you; you are asked to complete the attached form and return it to your post primary school, before 30th September. This form will be retained by the post-primary school and will be made available for inspection by authorised offices of the Department or from the Office of the Data Protection Commissioner.

The Department of Education and Skills is committed to respecting the privacy and confidentiality of all parents and guardians and their children's personal data and has taken all reasonable measures to do so.

Information which the Department stores on you or your child on its Post Primary Pupil Database is available to you. If you would like copy of these details please write to the

Parents' Learners and Database Section
Schools' Division
Cornamaddy
Athlone
Co. Westmeath.

You have the right to object to the processing of your or your child's personal data, to block certain uses of the data and also in the unlikely event that you identify any errors in the data held about you or your child, you have the right to correct such errors.

Further information on the October returns is available on the Department's website at www.education.ie (and search for October Returns).

Personal Data returned by Schools to the Department of Education and Skills, as part of their October Return, and which Data the Department of Education and Skills Shares with the Department of Social Protection, and is returned to solely assist the Department of Education and Skills Policy, Planning and Statistical Functions.

Personal Data Transferred to Department of Social Protection

Data Collected on each Student	**Purpose**
Personal Public Sector Number – PPSN collected for first time in 2001/02	Unique identifier for each student.
Student Name	Used to validate PPSN and also to identify students who have Irish Exemptions or studied Computer Studies. Also used to contact students if consent is needed to include them in educational surveys etc.
Student Home Address	
Date of Birth	There are minimum age threshold for students following different programmes.
Gender	Statistical analysis and to assist with individual student identity.
Mother's maiden name	PPSN validation. This is removed from the Department's records when confirmation of valid PPSN is received.

Other Personal Data Returned by Schools to the Department of Education and Skills necessary to identify a student as a recognised student, in accordance with the Rules and Programme for Secondary Schools.

Data Collected on each Student	**Purpose**
Previous school details	Used for statistical analysis and to ensure progression within the educational system is in accordance with the Rules and Programme for Secondary Schools
Programme – Junior, Leaving, PLC etc.	Used to establish if a student is following prescribed programmes as per Rules and Programme for Secondary Schools. For exam year students it is shared with the State Examination Commission to assist its preparation and organisation of State Examinations.
Subjects	
Subject Level	
Subject being taken through Irish	
Application for English Language Support (first sought in 2009/10)	Additional resources are provided to schools which have children in need of English Language Support

Data Collected on each Student	Purpose
Application for Traveller Support (first sought in 2009/10)	Additional teaching hours are provided for children who are members of the Traveller community. Written Consent is required by school authorities before they can include this in their returns to the Department.
Exemption from studying Irish	Irish is compulsory unless a student has obtained an exemption
Whether student is a boarder	Necessary for school funding considerations
Whether student is Repeating Leaving Certificate	Necessary for school funding considerations and the collection of Repeat Leaving Certificate fee
School Roll No.	Student must be enrolled in a school
Ab initio Indicator	Leaving Cert student may be doing a modern language at Junior Cert
Dispersed VTOS	Identified if student is following a course in this mode

Personal Data returned by Post Primary Schools to the Department to Assist with the Department's Policy, Statistical, Research and Planning Functions only.

Data Collected on each Student	Purpose
Country of Birth from 2009/10 onwards in earlier years Country of Origin	Used solely for statistical analysis
Medical Card Indicator – first sought in 2009/10	To aid the development of policy to promote social inclusion. Written Consent is required by school authorities before they can include this in their returns to the Department.
Reason for Irish exemption	Statistical analysis
Educational attainment	PLC students only for statistical analysis and development of educational policy in area of Further Education.
Date of leaving school	Early school leavers only for Retention Policy and Statistical analysis
Reason for leaving	For statistical and research purposes.

Schools also identify students by reference to being an exam entrant. This data assists the transfer of data on these students only to the State Examinations Commission, to assist its planning of state examinations.

Consent Form for Sensitive Personal Data for the School's October Return to the Department of Education and Skills

Certain sensitive personal data which the Department asks post-primary schools to furnish via the *"Annual Post-Primary School October Return/Examination Entries"* process requires your written consent for your child's school to record this information and for the school to forward this information to the Department for purposes as outlined in circular 0047/2010 a copy which is available at www.education.ie or on request from your child's school.

Please note that the reference to "you" in this consent form means a parent or a guardian of a student, or a student aged 18 years and over who is attending a recognised post-primary school.

Please enter the following details in BLOCK CAPITALS

Name of School: _____

Name of Parent/Guardian: _____

Name of Student: _____

Class year of student _____

1. Where your child is currently in 1st Year do you or your child possess a medical card?
   (please CIRCLE the appropriate answer)

   YES NO

2. Is your child a member of the Traveller Community *?
   (please CIRCLE the appropriate answer)

   YES NO

   * *"Traveller Community" means the community of people who are commonly called Travellers and who are identified (both by themselves and others) as people with a shared history, culture and traditions including, historically, a nomadic way of life on the island of Ireland. Section 2(1) of the Equal Status Act, 2000*

Signed: _____

Parent/Guardian/Student

Date: _____

Please complete this form and return to your post-primary school. This form will be retained by the post-primary school and will be made available for inspection by authorised officers of the Department or from the Office of the Data Protection Commissioner.

APPENDIX A
ACCS Guidelines on the Formulation of School Data Protection Policy

Data protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. Developments in information technology have led to an ever-increasing amount of personal information kept on computers about individuals. The ease of transfer and interchange of such information has given rise to an understandable concern that it may be used to the detriment of the individual concerned for purposes for which it was never intended. The Data Protection Act of 1988 gave new privacy rights to individuals and placed responsibilities on those who keep personal information on computers. The Data Protection (Amendment) Act of 2003 extended the scope of the Act to cover manual data also.

Schools are about people and the interactions between them. They bear a considerable responsibility and accountability for the development of young people, for the implementation of government policies and for the expenditure of state funds. They necessarily accumulate substantial amounts of personal information about pupils, parents, staff and management. It is therefore particularly important that appropriate policies and procedures are in place for the protection and proper use of all accumulated data and records.
The following is a list of current legislation, which guides and informs practice in the broad context of information management in schools:

- Data Protection Acts 1988 and 2003.
- Freedom of Information Act 1997 and 2003.
- Education Act 1998.
- Education Welfare Act 2000.
- Employment Equality Act 1998.
- Age of Majority Act 1985.
- Terms of Employment (Information) Act 1994 and 2001.
- EU Directive on Information and Consultation 2002/14/EC.
- Protection of Employees (Fixed Term Work) Act 2003.

Office of the Data Protection Commissioner (ODPC)
The Office of the Data Protection Commissioner is established under the Data Protection Acts in order to ensure that "Data Controllers" understand and meet their responsibilities under the Acts and to provide protection for the rights of individuals under the Acts. The Board of Management will normally be the Data Controller for the purposes of the Acts with the School Principal or Chairperson of the Board of Management acting as the contact person for any data protection issues raised with the Office of the Data Protection Commissioner. School staff are responsible to the school, in the first instance, for meeting data protection requirements.

Since 2007, following an amendment to registration requirements, schools are no longer required to register with the Office of the Data Protection Commissioner However, schools must still comply with the requirements of the Data Protection Acts in terms of how they handle personal data.

Contact details for the Office of the Data Protection Commissioner are as follows:
Office of the Data Protection Commissioner

Canal House
Station Road
Portarlington
Co. Laois
057 8684800
info@dataprotection.ie
www.dataprotection.ie

The Collection and Maintenance of Data.
In complying with the requirements of Data Protection legislation schools are expected to :

1. Obtain and process information fairly.
2. Keep it for one or more specified, explicit and lawful purposes.
3. Use and disclose it only in ways compatible with those 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.
8. Give a copy to an individual of his/her personal data on request.

Particular Issues which require consideration

Board of Management Records:

The School Board of Management is the ultimate authority in all matters relating to the management of the school. The records of its meetings form the definitive record of the schools decision-making process. It is important therefore that these records be prepared with care and kept safely and securely in a permanent archive.

School policy in this regard should provide that:

(i) Minutes of Board meetings should record attendance, items discussed and decisions taken. The views or contributions of named members of the Board to discussion should only be recorded at the specific request of the named member.

(ii) Minutes of each meeting, which have been approved by the Board and signed by its Chairperson and Secretary, should be filed and stored in an agreed manner. Two copies of Board of Management minutes should be sent to the Post Primary Administration Section, Department of Education and Science and one copy to the Post Primary Teachers' Section.

Copies of all correspondence raised at Board of Management meetings should be preserved in a permanent record with the Board of Management minutes.

Schools should also ensure information circulated for Board meetings containing personal data is done so securely and should be held in a confidential manner by each Board member. Equally, at the conclusion of a Board member's tenure or at shorter intervals, procedures should be in place to ensure the return or secure disposal of such information.

Confidentiality:
Board of Management business must be considered confidential to the members of the Board. It is equally important, however, that there be an open and transparent means

of communication between the Board and the members of the school community. It is recommended therefore that:

(i) Personal issues relating to pupils or staff members should always be considered confidential.
(ii) Provision be made for the Board to designate particular issues as confidential.
(iii) Provision be made for the reporting of matters which are not considered confidential by members of the Board to their nominating bodies.

It should be noted that Board of Management minutes, in so far as they are submitted to the DES may be subject to Freedom of Information demands at a later date by members of the public. Minutes are also subject, where they contain personal data, to release under an access request made under the Data Protection Acts by the person to whom the information relates or their parents if it relates to a pupil.

Employment Records:

The Board of Management is the employer of all teaching and non-teaching staff in the school. Recent employment legislation has placed considerable responsibility on employers in order to guarantee equality and fairness in the appointment and promotion of staff. Provision is made for any unsuccessful candidate for employment or promotion to appeal to a statutory Equality Appeals Tribunal or to an Employment Appeals Tribunal. In the case of teachers in Community and Comprehensive Schools there is, in addition, an agreed appeals process in relation to Post of Responsibility appointments.

In order to meet the legislative requirements and demands arising from possible appeals it is advisable that Boards of Management should retain the following in relation to every staff appointment or promotion:

- The decision of the Board of Management to make a particular appointment.
- The nature and the job description of the appointment to be made.
- The agreed method of advertisement for the position.
- A record of all applications and appropriate qualifications of candidates.
- The agreed procedure for interview and selection. (In the case of teaching appointments the decision to convene the approved Selection Board).
- The record and notes of short-listing, interview and agreed assessment procedures.
- The Report of the agreed order of merit of the candidates.
- The decision of the Board of Management to appoint.
- The letter of appointment.
- A signed contract of employment.

All of these records should be retained for as long as is required to answer any possible appeals that may occur.

Personnel Files.

It is recommended that a "personnel file" be maintained for each member of staff. This personnel file may contain:

- Original records of application and appointment to the post held.
- Record of appointments to promotion posts.
- Details of work record and noteworthy achievements.
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Records of any formal disciplinary actions taken by the school management. Staff members must be provided with copies of any such records and be

informed of their right to appeal against the inclusion of such record in their files.
- Any testimonials or references submitted or prepared on behalf of the staff member.

The school policy should explicitly state that all staff members have the right to inspect their own personnel files and the means by which they may exercise this right. A protocol should be agreed for the review of personnel files and for the removal of data which is no longer relevant.

Data Protection Clause for New Contracts of Employment

A statement such as the following could be included in a new employee's contract of employment to fulfil certain obligations under the Data Protection Acts, 1988 and 2003

> "*Upon joining the organisation, personal information will be requested from you in order that the organisation may effectively administer the agreement contained in this contract. For example, your P.P.S. number will be requested in order that income tax may be deducted from your salary, we will request confirmation of your date of birth, as it is required for pension purposes, and we will request your home contact details in case of emergency. All personal information regarding your employment will be held on computer and also in your personnel file. This information will not be disclosed to any external third party without your consent, except where necessary to comply with statutory requirements or where an organisation is acting on our behalf for example, the payroll administration supplier. You may, at any time, make a request for access to the information held about you as outlined in our Data Protection Policy.*
>
> *Any changes to your terms and conditions of employment will be notified to you in writing. Copies of these written memo's or e-mails will be kept on your hardcopy personnel file, and will also be recorded on our data base".*

Pupil Records.

It is recommended that a personal file be maintained for each pupil enrolled in the school. This file may contain:

- Information sought and recorded at enrolment – PPS number, address and contact details, names and addresses of Parents/Guardians, previous academic record, any relevant special conditions which may apply.
- Academic Record – subjects studied, class assignments, examination results as recorded on official school reports.
- Records of significant achievements.
- Records of disciplinary events and/or sanctions imposed.
- Records of attendance and punctuality.

Records of religious belief or background, racial or ethnic origin should be recorded only if they are clearly relevant e.g. the provision of religious instruction, the provision of special language teaching etc.

Reports of disciplinary events and academic record that are maintained in a student file should be recorded on **school-approved documentation designed within the school Code of Behaviour**. In order to ensure that no breach of propriety takes place,

schools are advised to consider an agreed code of appropriate and consistent written and spoken words in relation to pupil performance, behaviour and breaches of school codes. Discussions on this code should take place in the context of the school's Code of Behaviour.

Every effort should be made to liaise with primary school authorities to ensure that relevant student records, assessments, psychological reports are transferred with the pupil on enrolment. This should be done with the full knowledge and approval of parents and guardians. Similarly transfers of pupils between post-primary schools should include the transfer of pupil records, again with the full knowledge and approval of parents.

Attendance records

Particular obligations regarding records of pupil attendance arise from the Education (Welfare) Act, 2000. The National Education Welfare Board (NEWB) has provided guidelines for the collection, recording and reporting of these attendance records. School management is obliged to observe these guidelines.

Access to student files:

The school policy should state clearly:

- The procedures to be adopted for the maintenance and security of school files.
- The purpose or purposes to which information contained in the files may be put.
- The degree of access to those files by members of staff or others (e.g.: DES Officials, EWO, SENO, Gardaí, Health Officials etc). Any disclosure of information contained in files must only take place in compliance with Section 8 of the Data Protection Acts.
- Those who have the authority to add or remove items from the personal file.
- The length of time that information will be kept on file.

Parents and/or students who are over 18 years of age are entitled to, and should be facilitated in consulting their particular student file under the supervision of authorised school personnel.

School management should note that, under the Child Protection Guidelines for Post Primary Schools (DES 2004) it is stated that Public Bodies may refuse access to information obtained by them in confidence (Section 1.5.1)
The exceptions and exclusions that are relevant to child protection include the following:

(i) Protecting records covered by legal professional privilege
(ii) Protecting records which would facilitate the commission of a crime
(iii) Protecting records which would reveal a confidential source of information

(1.5.2 Child Protection Guidelines for Post Primary Schools)

Withholding the release of records requested under the Data Protection Acts can only be done having regard to the specific exemptions to the Right of Access as provided for in the Acts.

Information Returns to Department of Education & Science:

All returns of information to DES that include personal data should comply with the Data Protection Acts. Where required, the consent of parents/students must be secured before personal details are supplied to DES.

References/Testimonials:
The provision of both verbal and written references and testimonials to staff and to pupils presents significant demands on school administration in the context of legislation. Consideration should be given to the following when a request for a reference is made:

Staff:
A testimonial is a general appraising of an individual in either a professional or personal capacity.

A reference is a confidential letter of recommendation. References become the property of the individual to whom they are addressed and are usually more detailed and explicit than testimonials. Testimonials are a more general assessment of an individual in their professional competence and will become the property of the individual once given to that person. There is no obligation to write a reference for an employee or a student. Once written however it should be fair, accurate, factual, and free from bias or inequity. It may be wise from time to time to decline a reference or testimonial and if this is done no reason need be given. It is common practice to give a certificate of service or attendance and some detail as to the capacity in which one has known the applicant. This may be a wiser practice in some cases. Careless statements should be avoided. (See also ACCS Info 27/04, dated 16/06/04

Students
Applications for references or testimonials from students should be treated with equal caution to those of staff. Only authorised school personnel should give references and testimonials and the use of school headed notepaper should be carefully monitored. It is to be recommended that references or testimonials that are written and recorded in staff or pupil personal files should be countersigned by the Principal.

Financial Records:
There are extensive obligations on Boards of Management to maintain records of income and expenditure, class maintenance, stock records. School Policy should note the obligation of the Board of Management to meet the requirements of the "Financial Guidelines For Community and Comprehensive Schools" as published by the Department of Education and Science.

For how long should records be kept?
In general personal data should not be kept for any longer than is necessary to fulfil the function for which is was first recorded. The length of time involved in particular cases can be a matter of debate. However, school policy should indicate the length of time for which particular records may be kept and indicate the ways and means by which individual members of staff or students may seek a change of policy in this regard.

Some statutory requirements should be noted:
1. There is a statute of limitations of 3 years relating to personal injuries which, in the case of a minor, is dated from his/her 18th birthday. Consequently it is suggested that relevant information in student files should be kept for a period of 5

years after each particular Year Group has completed Leaving Certificate. Information which might be pertinent to an allegation of abuse should be retained indefinitely.

2. Tax and Pay Records should be kept indefinitely.

3. Employment Legislation sets out some time limits, which **must** be observed:

ACT	Record Keeping
Organisation of Working Time Act	3 years
1997	1 years
Employment Equality Act	3 years
Minimum Wage	10 years
Health and Safety	1 years
Maternity Leave	1 years
Adoptive Leave	3 years
Carer's Leave	8 years
Parental Leave	1 years
Unfair Dismissals	6 months
Redundancy Payments	3 years
Collective Redundancies	

4. Reports relating to accidents involving school personnel or occurring on school property should be recorded and retained in accordance with guidelines from the State Claims Agency, the Health and Safety Authority, and the Department of Education and Science.

Electronic Data Security

Section 2(1)(d) of the 1988 Act places an obligation on Data Controllers and/or Data Processors to have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction."

It is a matter for each school to evaluate its needs in this regard and to set down guidelines for staff on the measures to be adopted to safeguard the data under its control. When determining measures, a number of factors need be taken into account:

- The state of technological development;
- The cost of implementing measures;
- The harm that might result from unauthorised or unlawful processing; in a school context where sensitive personal data is being processed, security safeguards would have to take due account of this;
- The nature of the data concerned;

It is advisable that technical assistance be employed in designing these security measures. It is essential that management refers to information which is available on the ODPC website at www.dataprotection.ie (copy attached, appendix 2)

Conducting a Data Protection Audit.

Boards of Management have an obligation to conduct periodic audits of their Data Protection procedures. In doing so the following procedure is recommended:

1. Appoint a Compliance Officer
2. Evaluate current practices and procedures to ensure that they meet the demands of the Acts

3. Conduct a risk assessment by
    - Examining personnel files and evaluating the data (e.g. recruitment, disciplinary, leave of absence, health,)
    - Examining all systems containing personal data
    - Consider the location of any other data held
    - Remove out of date and update inaccurate data
    - Evaluate who has access to data
4. Advise employees
    - How access is made available
    - Of the purpose for which data is held
    - To whom data may be disclosed
    - The source of data

5

Processing of Personal Data in other contexts, e.g. CCTV, Use of Biometric Systems:

Use of CCTV Systems in Schools:

The use of CCTV systems involves the processing of personal data and so any system must operate in compliance with the Data Protection Acts. In a school context consideration of the matter involves having regard to the rights of staff and students in relation to the processing of their personal data. While the principle concern for the installation of such systems can primarily be for security purposes, no data protection concerns would arise in relation to the deployment of cameras along the perimeter of a school building. Any use beyond this (i.e. internally) would need to be fully justifiable and evidence-based with a very high threshold for such evidence. This is particularly relevant in a place of education because such recording would consist of the personal information of both staff and students. In this respect, the Data Protection Commissioner has issued advice that should his Office receive any complaints in relation to the operation of CCTV in schools that this will be the criteria by which he will assess the proportionality of such use and form an opinion on whether the provisions of Section 2(1)(c)(iii) of the Acts have been breached. A guidance note on the use of CCTV systems is included at Appendix 3.

Use of Biometric Time and Attendance Systems in Schools:

The guidance note available at Appendix 4 has been prepared by the Office as the Data Protection Commissioner as an aid to schools, colleges and other educational institutions that may be considering the installation and use of a biometric system. This document is intended to encourage such institutions to fully consider if there is need for a biometric system in the first place and then to assess the privacy impact of different systems.

The critical issues to be considered from a data protection perspective are the proportionality of introducing a biometric system and the requirement to obtain the signed consent of the student users (and their parents or guardians in the case of minors) giving them a clear and unambiguous right to opt out of the system without penalty.

The document is not intended to promote any particular system, but is intended to make schools and colleges aware of their responsibilities under the Data Protection Acts 1988 & 2003. It is the use of a biometric system that may give rise to a data protection concern, not necessarily the production or sale of a system. All situations must be judged on a case-by-case basis.

Appendix 1

Statement of Data Protection Policy which may be issued to all employees and students

The school is committed to adhere to the provisions of the Data Protection Acts 1988 and 2003, and in so doing to afford adequate protection to all employees and students with regard to their personal information held by the school.

A personal file is created for each student and employee, both on computer and in hard copy form. This file contains personal information and as such is subject to the regulation of the Data Protection Acts 1988 and 2003. In order to comply with the legislation, and ensure that personal information is kept in a safe manner which secures its confidentiality, the school adheres to the data quality principles as set out in the Data Protection Acts, 1988 and 2003 and guidance notes issued by the Data Protection Commissioner's Office. All personal information will be processed in a manner that complies with the following Data Quality Principles;

- Information will be obtained and processed fairly.
- All persons are made aware of the purpose for which information is kept.
- The information is only disclosed in a manner consistent with its purpose, and to recipients as agreed with the employee/student (or his/her parent/guardian).
- The information is kept safe and secure, and those working with the information are trained as to their responsibilities in this regard.
- The organisation undertakes to keep the information accurate, up-to-date and complete.
- Information held is adequate and relevant, and not excessive, and regular reviews are carried out to ensure that where this is not the case, information will be destroyed as outlined in the organisations security policy.
- Information will only be retained for as long as required to complete the purpose specified for such information.
- Should any person request access to their file; this access will be granted within a maximum of 40 days of receipt of a written request.
- Viewing of all files will take place under the supervision of authorised school personnel.

Appendix 2

Extract from the website of the Data Protection Commissioner
www.dataprotection.ie (Go to Guidance Material/Security Guidelines)
This guidance section should be replaced with the updated security guidelines available at the link below:

http://www.dataprotection.ie/docs/Security_Guidelines/29.htm

Security Guidelines

The Data Protection Acts, 1988 and 2003 do not detail specific security measures that a Data Controller or Data Processor must have in place. Rather section 2(1)(d) of the 1988 Act places an obligation on persons to have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction."

SI 626 of 2001, and later the Data Protection (Amendment) Act, 2003, introduced a new section 2C into the 1988 Act. This section helps interpret the nature of security measures required to demonstrate compliance with 2(1)(d). When determining measures, a number of factors need be taken into account:

- The state of technological development;
- The cost of implementing measures;
- The harm that might result from unauthorised of unlawful processing;
- The nature of the data concerned;

A further development introduced by the 2003 Act is the obligation on data controllers and data processors to ensure that their staff are aware of security measures and comply with them. This guidance is purely intended as an indication of issues which data controllers and data processors may wish to consider when developing security policies.

Access Control

The obligation to prevent unauthorised access to data can, at the simplest level, be met by placing a password onto a computer. This would certainly be the minimum measure acceptable. However, it is only effective if staff keep the password secure, and is reviewed and changed if necessary. A password is one, simple, form of authentication. A more advanced form is the use of a token (such as a smart card), or the use of biometrics (such as an iris scan or a finger print scan). Where all three are used in combination, this would offer a high level of authentication.

Network administrators can add a level of security beyond mere authentication. Users tend to develop unique profiles, depending on what they normally do on their computers. This can be a combination of the time and frequency of access; location; nature of data accessed. Where a user seeks to access data in an unusual manner,

which conflicts with an established profile, a challenge response question can be asked by the system. This type of authentication prevents a person who has found a password from accessing the system.

In conjunction with authentication, the nature of access allowed to an individual user should be set and reviewed on a regular basis. Ideally, users should only have access to data which they require in order to perform their duties. Regular reviews are necessary in order to increase if necessary as well as to restrict previous access where a user role changes.

A logging and reporting system can be a valuable tool in assisting the network administrator in identifying abuses and developing appropriate responses.

Encryption

There are a variety of tools available with which to encrypt data. These can be useful in closed systems, where all users can have access to the key with which to decrypt data. Providing such a key is held securely, encryption offers a high degree of protection against external attack.

Where encryption currently does not work satisfactorily is in sending data to the outside world. Use of a Public Key Infrastructure (PKI) requires that both sender and recipient use the same encryption system. Until such time as a market leader or industry standard exists, such PKI's will be slow to develop.

Anti-Virus Software

Anti-Virus software is not only required to prevent infection from the internet (either e-mail or web-sourced). Viruses may also be introduced from diskettes or CD's. No anti-virus package will prevent all infections, as they are only updated in response to infections. It is essential that users update such software on a regular basis, but also keep vigilant for potential threats. A policy of not opening e-mail attachments from unexpected sources can be a useful way of preventing infection.

Firewalls

A firewall is useful where there is any external connectivity, either to other networks or to the internet. It is important that firewalls are properly configured, as they are a key weapon in combating unauthorised access attempts. As firewalls are available for free download from the internet, they should routinely be installed by all data controllers and processors. This will become more important as persons progress to "always-on" internet connections, exposing themselves to a greater possibility of attack.

Automatic screen savers

Most systems allow for screensavers to activate after a period of inactivity, on the computer. This automatic activation is useful as the alternative manual locking of a workstation requires positive action by the user every time he/she leaves the computer unattended. Regardless of which method an organisation employs, computers should

be locked when unattended. This not only applies to computers in public areas, but to all computers. It is pointless having an access control system in place if unattended computers may be accessed by any staff member.

Logs and Audit trails

It is of course pointless having an access control system and security policy of the system cannot identify any potential abuses. Consequently, a system should be able to identify the user name that accessed a file, as well as the time of the access. A log of alterations made, along with author/editor, should also be created. Not only can this help in the effective administration of the security system, its existence should also act as a deterrent to those staff tempted to abuse the system.

The Human Factor

No matter what technical or physical controls are placed on a system, the most important security measure is to ensure that staff are aware of their responsibilities. Passwords should not be written down and left in convenient places; passwords should not be shared amongst colleagues; unexpected e-mail attachments should not be opened unless first screened by anti-virus software.

IS17799 Certification

The National Standards Authority of Ireland has set a standard for information security management systems. If a body is certified to be IS17799 compliant, it would demonstrate compliance with the security requirements of the Data Protection Acts, 1988 & 2003.

Further information on IS 17799 may be found on the NSAI website.

Remote Access

Where a worker is allowed to access the network from a remote location (e.g. From home or from an off-site visit), such access is creating a potential weakness in the system. Therefore, the need for such access should be properly assessed and security measures reassessed before remote access is granted.

Wireless networks

Access to a server by means of a wireless connection (such as infrared or radio signals) can expose the network to novel means of attack. The physical environment in which such systems are used may also be a factor in determining any weakness in the system security. As with remote access, wireless networks should be assessed on security grounds rather than solely on apparent ease of use.

Laptops

Laptops, personal organisers and other form of portable computers are especially vulnerable, as there is not only a higher risk of theft, but also a new risk of accidental loss. It would be a sensible precaution not only to have adequate security measures,

but also to limit what data are places on such machines in the first place. If practical, collected data should be downloaded at an early date with administrators reviewing the nature and quantity of data held.

Where laptops are the personal property of an individual, the data controller should have a contract in place to detail the conditions under which data may be processed on personal computers. A contract might also be advisable to cover all employee use of portable computers, especially concerning use of data where a person leaves the employment of a data controller.

Even where data are not routinely deleted from portable computers, such data should be backed up onto the network. This will assist in keeping the data on the network accurate and up to date, as well as defending against the accidental loss or destruction of data on portable computers.

Back-up systems

A back up system is an essential means of recovering from the loss or destruction of data. While some system should be in place, the frequency and nature of back up will depend, amongst other factors, on the organisation concerned and the nature of data being processed. The security standards for back-up data are the same as for live data.

Physical Security

Physical security includes issues like perimeter security (office locked and alarmed when not in use); computer location (so that the screen may not be viewed by members of the public); disposal (so that computer print outs containing sensitive data are securely disposed of).

Appendix 3:

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

Appendix 4:

Biometrics in Schools, Colleges and other Educational Institutions

The following guidance has been prepared as an aid to schools, colleges and other educational institutions that may be considering the installation and use of a biometric system. This document is intended to encourage such institutions to fully consider if there is need for a biometric system in the first place and then to assess the privacy impact of different systems.

The critical issues to be considered from a data protection perspective are the proportionality of introducing a biometric system and the requirement to obtain the signed consent of the student users (and their parents or guardians in the case of minors) giving them a clear and unambiguous right to opt out of the system without penalty.

The document is not intended to promote any particular system, but is intended to make schools and colleges aware of their responsibilities under the Data Protection Acts 1988 & 2003. It is the use of a biometric system that may give rise to a data protection concern, not necessarily the production or sale of a system. All situations must be judged on a case-by-case basis.

1. Different types of Biometric systems

All biometric systems operate on the basis of the automatic identification or authentication/verification of a person. What differs between systems is the nature of the biometric and the type of storage.

1.1 Information used to generate biometric data

Biometric data may be created from physical or physiological characteristics of a person. These include a fingerprint, an iris, a retina, a face, outline of a hand, an ear shape, voice pattern, DNA, and body odour. Biometric data might also be created from behavioural data such as hand writing or keystroke analysis. Generally, a digitised template is produced from the biometric data. This template is then compared with one produced when a person presents at a reader.

1.2 Types of biometric data

There are three principal types of biometric data:

• Raw Images, consisting of recognisable data such as an image of a face or a fingerprint, etc.

• Encrypted images, consisting of data that can be used to generate an image.

• Encrypted partial data, consisting of partial data from an image, which is encrypted and cannot be used to recreate the complete original image.

1.3 Types of Biometric systems

There are two principal types of systems:

• Identification systems, which confirm the identity of an individual;

• Authentication / verification systems, which confirm that a biometric derived from a person who presents at a reader matches another biometric, typically stored on a card and presented simultaneously.

1.4 Storage of biometric data.

There are two principal methods of storing biometric data/templates:

• Central databases store the templates on a central system which is then searched each time a person presents at a reader.

• A card is used to store a template. A template is generated when a person presents at a reader, and this template is compared with the template on the card.

Data Protection issues concerning biometrics.

2. Proportionality

Section 2(1)(c)(iii) of the Data Protection Acts states that data

"shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed."

The key word here is "excessive." Accordingly, the first question to be asked when considering the installation of such a system is what is the need for it? What is wrong with current systems or less invasive alternatives?

As individuals have fundamental Human Rights which are protected by the Data Protection Acts, a school or college must conduct some assessment of the need for a biometric system and an evaluation of the different types of available systems before the introduction of any particular system.

Determining what is excessive requires a case-by-case analysis. Some factors which may be taken into account include:

• Environment. Does the nature of the school or college require high levels of security? Are there areas of the campus which contain sensitive information, high value goods or potentially dangerous material which may warrant a higher level of security than would areas with low value goods or areas with full public access? Of course such a consideration would also point towards all persons working in the environment being similarly required to use the biometric system.

• Purpose. Can the intended purpose be achieved in a less intrusive way? A biometric system used to control access for security purposes in certain areas of the campus might be legitimate while a biometric system used by the same school or college purely for attendance management purposes might not.

• Efficiency. Ease of administration may necessitate the introduction of a system where other less invasive systems have failed, or proved to be prohibitively expensive to run.

• Reliability. If a school or college suffers as a result of students impersonating each other for various reasons, then a system could possibly be justified as long as other less invasive ones have been assessed and reasonably rejected.

3. Fair obtaining and processing.

Section 2(1)(a) of the Acts require that

"The data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly."

In order to demonstrate compliance with this provision, at least one of the provisions of Section 2A of the Acts must be met. In the context of the introduction of a biometric system for use by students in a school or college, these include:

• Consent, and

• Legitimate interests of the school or college: where the processing is necessary for the purposes of the legitimate interests pursued by the school or college or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Consent: In the context of students attending a place of education, the Data Protection Commissioner would stipulate that the obtaining of consent is of paramount importance when consideration is being given to the introduction of a biometric system. It is the Commissioner's view that when dealing with personal data relating to minors, the standards of fairness in the obtaining and use of data, required by the Data Protection Acts, are much more onerous than when dealing with adults. Section 2A(1)(a) of the Data Protection Acts states that personal data shall not be processed by a data controller unless the data subject has given his/her consent to the processing, or if the data subject by reason of his/her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian etc. While the Data Protection Acts are not specific on what age a subject will be able to consent on their own behalf, it would be prudent to interpret the Acts in accordance with the Constitution. As a matter of Constitutional and family law a parent has rights and duties in relation to a child. The Commissioner considers that use of a minor's personal data cannot be legitimate unless accompanied by the clear signed consent of the child and of the child's parents or guardian.

As a general guide, a student aged eighteen or older should give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. (Consent may not be considered to be in place for students in this age bracket unless it is given by both the student and a parent/guardian). In the case of children under the age of twelve, consent of a parent or guardian will suffice. Consent

to the use of a biometric system in places of education should be obtained by means of a positive opt-in on the part of students (and/or their parents or guardians as set out above). An audit trail of the opt-ins should be maintained by the data controller for the duration of each student's enrolment. All students (and/or their parents or guardians as set out above) should, therefore, be given a clear and unambiguous right to opt out of a biometric system without penalty. Furthermore, provision must be made for the withdrawal of consent which had previously been given.

Legitimate interests: Whilst the "legitimate interest" provision may seem appealing, it requires that a balance be struck. What is acceptable in one case may not be acceptable in another and a school or college seeking to rely upon this provision must take into account the potential effect upon student privacy rights. In any event, the Data Protection Commissioner considers that, in the context of a student environment, the processing of personal data using a biometric system would be prejudicial to the fundamental rights and freedoms of the students concerned in the absence of freely given consent.

3A. Fair obtaining of sensitive data.

If a biometric identifies sensitive data (such as data relating to a student's health or facial appearance thereby revealing race), at least one provision of section 2B of the Acts must be met in addition to those mentioned above. In the context of the introduction of a biometric system for use by students in a school or college, these provisions include:

• consent explicitly given.

• necessary processing for the performance of a function conferred on a person by or under an enactment.

Explicit consent: As stated above, all students (and/or their parents or guardians) should be given a clear and unambiguous right to opt out of a biometric system without penalty. The same consent which applied to the principle of obtaining and processing data fairly also applies to the fair obtaining of sensitive data.

Necessary for the performance of a function conferred under an enactment: Any legal obligation to record the attendance of students need not, in itself, require a biometric system to satisfy. For example, the Education (Welfare) Act, 2000 requires schools to maintain a record of the attendance or non-attendance on each school day of each student registered at the school. This requirement does not specify how the attendance

data should be obtained. The key word in this provision of the Data Protection Acts concerning the processing of sensitive personal data is "necessary." It is the view of the Data Protection Commissioner that the processing of sensitive personal data through use of a biometric system is not necessary to meet the requirements of the Education (Welfare) Act, 2000 in respect of recording student attendance. There are several long established and successful alternative methods of recording student attendance at schools which do not require the processing of a student's sensitive personal data.

4. Transparency

Section 2D of the Acts require that a school or college provide at least the following information to students when processing their data:

• The identity of the data controller in the school or college.

• The purpose in processing the data.

• Any third party to whom the biometric data will be given.

It is essential that students are aware of the purpose for which the biometrics data will be processed. This means that a school or college must carefully think through any purpose or potential purpose. Is the system solely for attendance management purposes? Will it be used for access control? What are the consequences for the student concerned if there is an identified abuse of the system? Under what circumstances will management access logs created by the system?

Transparency is even more important where the biometric system does not require the knowledge or active participation of a student. A facial recognition system, for instance, may capture and compare images without that person's knowledge.

5. Accuracy

Section 2(1)(b) of the Acts require that data shall be

"Accurate and complete and, where necessary, kept up to date."

Any biometric system must accurately identify the persons whose data are processed by the system. If changes in physical or physiological characteristics result in a template becoming outdated, a procedure must be in place to ensure that the data are kept up to date.

6. Security

The requirement, under section 2(1)(d), that a school or college has appropriate security measures in place to prevent the unauthorised access to, or the unauthorised alteration, disclosure or destruction of data would appear to promote the use of technological solutions such as encryption.

However, in deciding upon what constitutes an appropriate security measure, Section 2C details four factors that should be taken into account:

• The state of technological development.

• The cost of implementing such technology.

• The nature of the data being protected.

• The harm that might result through the unlawful processing of such data.

A minimum standard of security would include:

• Access to the information restricted to authorised staff on a 'need to know' basis in accordance with a defined policy.

• Computer systems should be password protected.

• Information on computer screens or manual files should be hidden from persons who are not authorised to see them.

• A back-up procedure for computer held data, including off-site back-up.

• Ensuring that staff are made aware of the school or college's security measures, and comply with them.

• Careful disposal of documents such as computer printouts, etc.

• The designation of a person with responsibility for security and the periodic review of the security measures and practices in place.

• Adequate overall security of the premises when it is unoccupied.

• Where the processing of personal data is carried out by a data processor on behalf of the school or college, a contract should be in place which imposes equivalent security obligations on the data processor.

7. Retention

Section 2(1)(c)(iv) of the Data Protection Acts provides that data shall not be kept for longer than is necessary for the purpose. In the context of a biometric system in a school or college, it would be necessary to devise a retention policy in advance of the deployment of the system which clearly sets out the retention period which would apply to biometric data. The Data Protection Commissioner would expect that as soon as a student permanently leaves the school or college, his/her biometric data would be immediately deleted.

8. Privacy Impact Assessment.

The Data Protection Commissioner cannot give a general approval or condemnation of biometric systems. Each system must be judged in respect of the situation in which it is used. A case-by-case judgement is required. With that in mind, the Commissioner encourages schools and colleges to take the above guidance into account if considering introducing any biometric system.

Before a school or college installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out. A school or college which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against a school or college by the Commissioner, or may expose a school or college to a claim for damages from a student. Data protection responsibility and liability rests with the school or college, not with the person who has supplied the system (where that person also acts as a data processor on behalf of the employer, it will have its own separate data protection responsibilities in relation to the security of the data).

Some of the points that might be included in a Privacy Impact Assessment are:

Do I have an attendance management and/or access control system in place?

Why do I feel I need to replace it?

What problems are there with the system?

Are these problems a result of poor administration of the system or an inherent design problem?

Have I examined a number of types of system that are available?

Will the non-biometric systems perform the required tasks adequately?

Do I need a biometric system?

If so, which kind do I need?

Do I need a system that identifies students as opposed to a verification system?

Do I need a central database?

If so, what is wrong with a system that does not use a central database?

What is the biometric system required to achieve for me?

Is it for attendance management purposes and/or for access control purposes?

How accurate shall the data be?

What procedures are used to ensure accuracy of data?

Will the data require updating?

How will the information on it be secured?

Who shall have access to the data or to logs?

Why, when and how shall such access be permitted?

What constitutes an abuse of the system by a student?

What procedures shall I put in place to deal with abuse?

What legal basis do I have for requiring students to participate?

How will I obtain the consent of the existing students (or their parents/guardians if applicable)?

How will I obtain the consent of new students (or their parents/guardians) who will enrol at a future date?

How will I ensure that students will be given a clear and unambiguous right to opt out of a biometric system without penalty?

What procedures will I put in place to provide for the withdrawal by students of consent previously given?

What system will I put in place for students who opt out of using the biometric system?

How will I ensure that students who are unable to provide biometric data, because of a disability for example, are not discriminated against by my school or college by being required to operate a different system, or otherwise?

Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?

If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?

If the introduction of a biometric system is justified, can I offer an alternative system to individuals who may object to the invasion of privacy involved in a biometric system?

What is my retention policy on biometric data?

Can I justify the retention period in my retention policy?

How shall I inform students about the system?

What information about the system need I provide to students?

Would I be happy if I was a student asked to use such a system?

Am I happy to operate a biometric system in an educational establishment where the use of such a system can make students less aware of the data protection risks that may impact upon them in later life?

Does my school or college have a comprehensive data protection policy as required by the Department of Education and Science since 2003?

Have I updated this policy to take account of the introduction of a biometric system for use by students?