



Monkstown Educate Together
National School

Data Protection Policy

Monkstown Educate Together NS

April 2016

TABLE OF CONTENTS

Introductory Statement	3
Scope	3
<i>Purpose of the Policy</i>	3
<i>Definition of Data Protection Terms</i>	3
Rationale	4
<i>Other Legal Obligations</i>	4
Relationship to Characteristic Spirit of Monkstown Educate Together	6
Goals/Objectives	6
Key Measures/Content of Policy	6
A. <i>Details of all personal data which will be held, the format in which it</i> <i>will be held and the purpose(s) for collecting the data in each case</i>	7
B. <i>Details of the arrangements in place to ensure compliance with</i> <i>the eight rules of data protection</i>	12
Links to Other Policies and to Curriculum Delivery	12
Implementation Arrangements, Roles and Responsibilities	12
Ratification and Communication	13
Monitoring and Implementation of the Policy	14
Reviewing and Evaluating the Policy	14
APPENDICES	15
Appendix 1	15
Appendix 2	16
Appendix 3	22

Introductory Statement

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

The policy applies to all school staff, the Board of Management, Parents/Guardians, students and others (including prospective or potential students and their Parents/Guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Scope

Purpose of the Policy

The Data Protection Acts 1988 and 2003 apply to the keeping and processing of Personal Data, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their Parents/Guardians how their data will be treated.

The policy applies to all school staff, the Board of Management, Parents/Guardians, students and others (including prospective or potential students and their Parents/Guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

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

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

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

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

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

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

Data Controller for the purpose of this policy is the Board of Management represented by the Chairperson, Board of Management, Monkstown Educate Together N.S.

Rationale

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

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

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

Other Legal Obligations

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

For example:

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School
- Under section 20(5) of the Education (Welfare) Act, 2000, a Principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the Principal of another school to which a student is transferring

- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day
- Under Section 28 of the Education (Welfare) Act, 2000, the school may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, Túsla other schools, other centres of education) provided the School is satisfied that it will be used for a “relevant purpose” (which includes recording a person’s educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)
- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers (“SENOS”) such information as the Council may from time to time reasonably request
- The Freedom of Information Act 1997 provides a qualified right to access information held by public bodies which does not necessarily have to be “personal data” as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body
- Under Section 26(4) of the Health Act, 1947 a school shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to Characteristic Spirit of Monkstown Educate Together

Monkstown Educate Together (METNS) is committed to the ethos and values of our patron body, Educate Together.

Our METNS school community is committed to fostering a school environment that is:

- A place where we are welcomed and in turn are welcoming of others
- A place where we are treated with respect and in turn treat others respectfully
- A place where we feel happy and safe
- A place where we are encouraged to achieve our full potential
- A place where our self esteem and self-confidence can flourish
- A place of quality teaching and learning
- A place where a love of learning is nurtured
- A place where we can be ourselves and in turn allow others to be themselves

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

Goals/Objectives

In this policy, METNS strives:

- To ensure that the school complies with the Data Protection Acts
- To ensure compliance by the school with the eight rules of data protection as set down by the Data Protection Commissioner based on the Acts (see below, B)
- To ensure that the data protection rights of students, staff and other members of the school community are safeguarded

Key Measures/Content of Policy

- A. Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data in each case.**
- B. Details of the arrangements in place to ensure compliance with the eight rules of data protection.**
- A. Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data in each case.**

Staff records:

Categories of staff data: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures)

Purposes: Staff records are kept for the purposes of:

- The management and administration of school business (now and in the future)
- To facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- To facilitate pension payments in the future
- Recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- To enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- To enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies and for compliance with legislation relevant to the school

Location and Security:

- In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access
- The records of staff members current and former are kept in manual and digital format in personal files and in digital format as an On-Line Claims System (OLCS provided by Department of Education and skills (DES))
- Manual files are retained in the Principal's office. The Principal, Deputy Principal, secretary(s) and Chairperson (as Data Controller) only, will have access to those files which will contain information solely related to professional matters

- Digital files are retained on the school computer (currently in the secretary's office) and are protected by password known only to the chairperson, (as Data Controller) the secretary, the deputy Principal and the Principal. These records will be retained in the school. Certain data may be held in cloud storage that is no less secure than the data held on the school computer

B. Student/Pupil records:

Categories of Student/Pupil data: These may include information which is sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:

- Name, address and contact details, PPS number
- Date and place of birth
- Names and addresses of Parents/Guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
- Membership of the Travelling Community, where relevant
- Whether English is the student's first language and/or whether the student requires English language support
- Any relevant special conditions (e.g. Special Educational Needs, health issues etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students.
- Academic records – subjects studied, class assignments, examination results as recorded on official school reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents
- Records of any reports the school may have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures)

Purposes: The purposes for keeping student records are:

- To enable each student to develop to their full potential
- To comply with legislative or administrative requirements
- To ensure that eligible students can benefit from the relevant additional teaching or financial supports

- To enable Parents/Guardians to be contacted in the case of emergency or in the case of school closure or to inform parents of their child's educational progress or to inform parents of school events etc.
- To meet the educational, social, physical and emotional requirements of the student
- Photographs and recorded images of students are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's "Acceptable Usage" policy
- To ensure that the student meets the school's admission criteria
- To ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- To furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
- To furnish, when requested by the student (or their Parents/Guardians in the case of a student under 18 years) documentation/information/ references to second -level educational institutions (after enrolment)

Location and Security:

- All student records including Application/Enrolment Forms will be kept in a secure, locked filing cabinets that only personnel who are authorised to use the data can access
- Student attendance records (currently in Aladdin System) and PPS numbers will be maintained on the POD system from mid 2016 and will be maintained in line with DES Guidelines. Access will be by permission of the Principal or (when absent) Deputy Principal, to authorised personnel only
- Student attendance records, standardised test results, and end of year reports are kept on the Aladdin System and only personnel who are authorised to use the data can access it

Employees are required to maintain the confidentiality of any data to which they have access.

B. Board of Management Records

Categories of Board of Management data: These may include:

- Name, address and contact details of each member of the Board of Management (including former members of the Board of Management)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals

Purposes:

- To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

Location and Security:

- In a secure, locked filing cabinet and on the school computer system. It is protected by passwords known to the Principal and Chairperson of the BoM (as Data Controller). Only personnel who are authorised by the Chairperson or Principal to use the data, can access it.

Employees are required to maintain the confidentiality of any data to which they have access.

C. Other Records:

Records relating to contacts with outside agencies such as patron bodies /insurance companies/legal advisors/ etc. will be securely maintained in the manner appropriate to its origins e.g. paper correspondence or email as appropriate.

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database) as appropriate.

Creditors

Categories of data: the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- Name
- Address
- Contact details
- PPS number
- Tax details
- Bank details
- Amount paid

Purposes: This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

Location and Security: As with BoM records

Charity tax-back forms

Categories of data: the school may hold the following data in relation to donors who have made charitable donations to the school:

- Name
- Address
- Telephone number
- PPS number
- Tax rate
- Signature
- The gross amount of the donation.

Purposes: Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parent's name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.

Location: In a secure, locked filing cabinet in the secretary's office that only personnel who are authorised to use the data can access.

Security: The secretary, Principal, chairperson (As Data Controller) and Treasurer of BoM only will have access to these records as appropriate.

D. CCTV images/recordings

Categories: CCTV is installed at the front of the school, in the foyer, the corridors, at the back entrance, and in the car park. This CCTV system may record images of staff, students and members of the public who visit the premises.

Purposes: Safety and security of staff, students and visitors and to safeguard school property and equipment.

Location: Cameras are located as detailed above. Recording equipment is located in a locked cabinet in the downstairs corridor.

Security: Access to images/recordings is restricted to Chairperson of BoM, as Data Controller, the Principal & deputy Principal (in the absence of the Principal) and the caretaker. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

E. Assessments

Categories: The school will hold data comprising test results in respect of its students. These include class, mid-term, annual, continuous assessment.

Purposes: The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their Parents/Guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

Location and Security: As with student details; in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

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

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

1. Obtain and process information fairly
2. Keep it only for one or more 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.

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules 1 and 3 above is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner's website states the following:

"As a general rule in the area of education, a student aged eighteen or older may 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. In the case of students under the age of twelve consent of a Parent or Guardian will suffice".

Links to Other Policies and to Curriculum Delivery

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

The following policies are among those considered:

- Child Protection Policy
- Enrolment Policy
- Garda Vetting Policy
- Attendance Strategy
- Positive behaviour Policy/Anti-Bullying Policy
- Substance Use Policy
- Mobile Phone Policy
- Assessment Policy
- Learning Support and Special Education Policy
- ICT Acceptable Usage Policy
- Ethos Policy

Implementation Arrangements, Roles and Responsibilities

In Monkstown Educate Together the Chairperson of the BoM, on behalf of the BoM is the data controller, and the Principal is assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their Data Protection responsibilities.

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

Name:	Responsibility
Chairperson	Data Controller
Principal	Implementation of Policy
Teaching personnel: See current staff list	Awareness of responsibilities
Administrative personnel	Security, confidentiality
IT personnel	Security, encryption, confidentiality

Ratification and Communication

This Data Protection Policy is dated the 24th April 2016 for implementation from 1st June 2015. It was placed on the school website from September 2016 following consultation with Parents/Guardians, teaching and administrative staff and the pupils of METNS. All relevant personnel were made aware of their responsibilities under the policy by the BoM and the Principal.

All stakeholders concerned will be made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/Guardians and students are informed of the Data Protection Policy from the time of enrolment of the student by including reference to the Data Protection Policy as part of the Enrolment Pack, and by providing copies on request from the Secretary's office.

Monitoring and Implementation of the Policy

The implementation of the policy shall be monitored by the Principal and a sub-committee of the Board of Management consisting of a Parent/Guardian nominee and patron's nominee.

At least one annual report will be issued to the BOM by the Chairperson to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and Evaluating the Policy

This policy will be reviewed regularly according to the ongoing schedule of review of school policies.

Review may commence earlier in the light of guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), legislation and feedback from Parents/Guardians, pupils, school staff and others.

APPENDICES

Appendix 1

Data Protection Statement (METNS) for inclusion on relevant forms when personal information is being requested

The information collected on this form will be held by Monkstown Educate Together National School in manual and in electronic format. The information will be processed in accordance with the Data Protection Act, 1988 and the Data Protection (Amendment) Act, 2003.

The purpose of holding this information is for administration and to facilitate the school in meeting the student's educational needs etc.

Disclosure of any of this information to statutory bodies such as the Department of Education and Science or its agencies will take place only in accordance with legislation or regulatory requirements. Explicit consent will be sought from Parents/Guardians or students aged 18 or over if the school wishes to disclose this information to a third party for any other reason.

Parents/Guardians of students and students aged 18 or over have a right to access the personal data held on them by the school and to correct it if necessary.

I consent to the use of the information supplied as described.

Signed Parent/Guardian: _____

Signed Student: _____

Appendix 2

The following prompt questions should be regarded as a checklist in proofing the arrangements for adherence to each of the eight rules:

1. *Obtain and process information fairly: prompt questions*

- Are procedures in place to ensure that staff members, Parents/Guardians and students are made fully aware when they provide personal information of the identity of the persons who are collecting it, the purpose in collecting the data, the persons or categories of persons to whom the data may be disclosed and any other information which is necessary so that processing may be fair (as stated above, the sample statement in Appendix 1 could be included on relevant forms where personal information is being requested).
- Is personal information processed fairly in accordance with the Data Protection Acts, with consent being obtained from staff members, Parents/Guardians or students, where required? See *A Guide for Data Controllers* (pg. 7 and 8) for a list of exemptions from obtaining consent.
- Is sensitive personal information processed fairly in accordance with the Data Protection Acts, with explicit consent being obtained from staff members, Parents/Guardians or students, where required? See *A Guide for Data Controllers* (pg. 8) for a list of exemptions from obtaining consent.

2. *Keep it only for one or more specified, explicit and lawful purposes: prompt questions*

- Do the persons whose data is collected know the reason/s why it is collected and kept?
- Is the purpose for which the data is collected and kept a lawful one?
- Is school management aware of the different sets of data which are kept and the specific purpose of each?

3. *Use and disclose it only in ways compatible with these purposes: prompt questions*

- Is data used only in ways consistent with the purpose/s for which it was obtained?
- Is data disclosed only in ways consistent with that purpose?
- Is there a procedure in place, which is in accordance with the Data Protection Acts to facilitate the transfer of information to another school when a student transfers?

Note: Under Section 20 of the Education (Welfare) Act, 2000, each school Principal must maintain a register with the names of all children attending that school. When a child is transferring from the school, the Principal must notify the Principal of the new school of any problems relating to school attendance that the child concerned had and of any other matters relating to the child's educational progress that he or she considers appropriate. Under Section 28 of the Act, schools may supply personal data, or information extracted from such data, to other schools or another prescribed body if they are satisfied that it will be used in recording the student's educational history, monitoring the student's educational progress or developing the student's full educational potential. The bodies which have been prescribed (and so can share information) under Section 28 are:

- The Minister for Education and Science (which includes the Inspectorate and the National Educational Psychological Service (NEPS))
 - The National Council for Special Education (NCSE)
 - The National Educational Welfare Board (NEWB)
 - Each school recognised in accordance with section 10 of the Education Act, 1998
 - Each place designated by the Minister under section 10 of the Education Act, 1998 to be a centre for education.
-
- In what circumstances will personal data be disclosed to third parties, including the Department of Education and Science, the NEWB, Gardaí, in legal proceedings, HSE personnel etc.?
 - Is there a procedure in place, which is in accordance with the Data Protection Acts to facilitate the transfer of personal data abroad? See *A Guide for Data Controllers* (pg. 17).

Exceptions to disclosure rule:

- Data can be disclosed when required by law
- Data can generally be disclosed to an individual himself/herself or with his/her consent (see 8 below).

4. *Keep it safe and secure: prompt questions*

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

- Is access to the information (including authority to add/amend/delete records) restricted to authorised staff on a “need to know” basis?
- Who has access to what information based on this “need to know” policy?
- Are computer systems password protected?
- Is information on computer screens and manual files kept out of view of callers to the school/office?

- Are back-up procedures in operation for computer held data, including off-site back-up?
- Are all reasonable measure taken to ensure that staff are made aware of the security measures, and comply with them?
- Are all waste papers, printouts etc. disposed of carefully?
- Are steps taken to ensure that no unauthorised person can access data from computers which are no longer in use or subject to change of use?
- Is there a designated person responsible for security?
- Are there periodic reviews of the measures and practices in place?
- Are premises secure when unoccupied?
- Is there a contract in place with any data processor which imposes an equivalent security obligation on the data processor?

5. *Keep it accurate, complete and up-to-date: prompt questions*

- Are clerical and computer procedures adequate to ensure high levels of data accuracy?
- Are appropriate procedures in place, including periodic review and audit, to ensure that each data item is kept up-to-date?

Note: While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.

6. *Ensure that it is adequate, relevant and not excessive: prompt questions*

- Is the information held adequate in relation to the purpose/s for which it is kept?
- Is the information held relevant in relation to the purpose/s for which it is kept?
- Is the information held not excessive in relation to the purpose/s for which it is kept?

Note: While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.

7. *Retain it for no longer than is necessary for the purpose or purposes: prompt questions*

- Is a defined policy in place for the retention periods for all items of personal data kept?
- Are there management, clerical and computer procedures in place to implement such a policy?

Note: While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.

In general, personal data should not be kept for any longer than is necessary to fulfil the function for which it was first recorded. Retention times cannot be rigidly prescribed to cover every possible situation and schools need to exercise their individual judgement in this regard in relation to each category of records held. However, the following particular requirements should be met:

- School registers and roll books are required to be kept indefinitely within the school. Consideration is being given to amending the Data Protection Acts to allow schools to deposit completed school registers and roll books which are no longer required for administrative purposes with the Local Authority Archive Service. The Department will notify schools of any changes to the Acts in this regard.
- Pay, taxation and related school personnel service records should be retained indefinitely within the school.
- Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving school personnel/students or accidents occurring on school property), the relevant records should be retained until the possibility of litigation ceases.

Note: The statute of limitations in relation to personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their 18th birthday or later if the date of knowledge post dates their 18th birthday. While schools may wish to draw up their own policies as to how long to retain such records, it would appear prudent not to destroy records likely to be relevant in litigation at least until the **six year limitation period** has expired.

In line with the above, it is suggested that the information on student files might, as a general rule, be retained for a period of six years after the student has completed the Senior Cycle and/or reached the age of 18.

8. *Give a copy of his/her personal data to that individual on request*

On making an access request any individual (subject to the restrictions in Notes A and B below) about whom you keep personal data, is entitled to:

- A copy of the data which is kept about him/her
- Know the purpose/s for processing his/her data
- Know the identity of those to whom the data is disclosed
- Know the source of the data, unless it is contrary to public interest
- Know the logic involved in automated decisions
- A copy of any data held in the form of opinions, except where such opinions were given in confidence.

To make an access request, an individual must:

- Apply in writing
- Give any details which might be needed to help identify him/her and locate all the information you may keep about him/her

- Pay an access fee if the school wishes to charge one. The school need not do so, but if it does it cannot exceed the prescribed amount of €6.35.

There are a number of exceptions to the general rule of Right of Access, including those specified in Notes A and B below.

Handling access requests: prompt questions

- Is a named person responsible for handling access requests?
- Are there procedures in place to provide applicants with access to personal data about themselves in accordance with the Data Protection Acts as detailed above?
- Have criteria been set down on what is sufficient to prove identity in order to access personal data?

- Is there a procedure in place to record the outcome of any legal proceedings which may limit the right of one or both parents to access information about their child?

Note: If spouses are separated and one of them has obtained an order for custody but both of them remain guardians, then both of them are entitled to be involved in important decisions which affect the child.

- Are clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is made?
- Is there a procedure in place to rectify or erase any inaccurate information as identified by the individual on whom the data is kept, within 40 days of the request being made?
- Is information supplied promptly and within 40 days of receiving the request or, in respect of examinations data, within 60 days of receiving the request or 60 days of first publication of the results (whichever is the later)?
- Is the information provided in a form which is clear to the ordinary person?
- Is the individual informed within 40 days of the request if no information is held on them?
- Is the fee charged (if any) refunded to the individual if the request is not complied with or if it is necessary to rectify, supplement or erase the personal data concerned?

Note A: Access requests by students

- Students aged 18 and over are entitled to access their personal information in accordance with the Data Protection Acts.
- Students under 18 years of age can be given access to their personal information, depending on the age of the student and the nature of the record i.e. it is suggested that:
 - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
 - If the record is of a sensitive nature, it would be prudent to seek Parental/Guardian consent
 - if a student has some disability or medical condition that would impair his or her ability to understand the information, or if disclosure would be likely to be harmful to the individual concerned, parental/guardian consent should be sought.

Note B: Exceptions to note:

- Schools should note that Data Protection regulations prohibit the supply of:
 - Health data to a patient in response to a request for access if that would cause serious harm to his or her physical or mental health. The regulations also provide that such data is to be communicated only by, or after consultation with, an appropriate "health professional", normally the patient's own doctor
 - Personal data obtained in the course of carrying on social work if that would cause serious harm to the health or emotional condition of the data subject concerned. The regulations apply to social work carried on by Ministers, local authorities, the HSE or any other such bodies receiving financial assistance from public funds.

Appendix 3

Providing Information over the Phone

In Monkstown Educate Educate Together N.S. any employee dealing with telephone enquiries will be careful about disclosing any personal information held by the school over the phone. In particular the employee should:

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

Data will be retained/destroyed as per the Data Retention Schedule on www.dataprotectionschools.ie.