Ballymakenny College
Coláiste Bhaile Mhic Éinigh
An Educate Together and Louth Meath Education and Training Board parnership school

# Ballymakenny College Data Protection Policy

## 1. Introduction

In the course of its activities, Ballymakenny College accumulates substantial amounts of personal information about pupils, parents, staff and management. It is therefore particularly important that appropriate procedures are in place for the protection and proper use of all accumulated data and records.

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

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 information will be kept accurate, up-to-date and complete.
- The information will only be retained for as long as required to complete the purpose specified for such information.

The Principal shall, from time to time, administer a Data Protection Audit. Consideration shall also be given to security of information held on the school computer networks.

The school is not, however, required to register with the Office of the Data Protection Commissioner.

**Key Areas**
**Board of Management**
**Employment Records**
**Personnel Files**
**Pupil Records**
**Parent Records**
**References**
**Financial records**
**Reports relating to accidents involving school personnel**.

## 1. Board of Management Records

The Principal acting as Secretary to the Board of Management shall store the Minutes of Board meetings securely in the Principal's office.

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. However, there shall be an open and transparent means of communication between the Board and the members of the school community, and provision is made for the reporting of matters which are not considered confidential by members of the Board to staff, the Parents' Association Committee and the Student Council.

(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.

**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.

## 2. Employment Records

The Board of Management, as the employer of all teaching and non-teaching staff in the school, shall 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.

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

## 3. Personnel Files

A "personnel file" is maintained for each member of staff. This personnel file shall 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.

Hard copies of Personnel Files shall be held securely in the Principals Office.

Staff members shall 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.

Upon joining Ballymakenny College, personal information will be requested from staff in order that the school may effectively administer the employment of the teacher. This may include:
(i) the teacher's P.P.S. number
(ii) confirmation of the teacher's date of birth
(iii) home and mobile contact details in case of emergency

**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".*

All personal information regarding a teacher's employment will be held on computer and also in the teacher's personnel file. This information will not be disclosed to any external third party without the teacher's consent, except where necessary to comply with statutory requirements or where an organisation is acting on the school's behalf for example, the payroll administration supplier.

A staff member may, at any time, make a request for access to the information held about them. All staff members have the right to inspect their own personnel file within seven working days of the submission of a written request to do so. Viewing of all files will take place under the supervision of the Principal or other authorised school personnel.

**4. Pupil Records**

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.

Hard copies of Pupil Records shall be held securely in the Secretary's Office.

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

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.

***Attendance records***

Particular obligations regarding records of pupil attendance arise from the Education (Welfare) Act, 2000. Ballymakenny College School follows the guidelines issued by the National Education Welfare Board (NEWB) for the collection, recording and reporting of these attendance records.

***Access to student files***

The student files are maintained by the Clerical Officer of the school, who is responsible for their security. Teachers may access, and add to, these files if it is considered to be in the interest of the student, and the information contained therein may be released to other parties (e.g.: DES Officials, NEWB, SENO, Gardaí, Health Officials etc) at the discretion of the Principal.

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)

**5. Parent Records**

The school does not keep personal files for parents or guardians. However, information about, or correspondence with, parents are included in the files for each student. This information shall be treated in the same way as any other information in the student file and may be accessed similarly.
The school keeps financial records which include records of fees paid and unpaid and any payments of the Voluntary Contribution. These records are administered by the Clerical Officer and are treated as strictly confidential. Parents are entitled to contact the school to seek details of their financial record, and shall be facilitated in such a way that the financial record of no other parent or family is divulged.

**6. References**

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.

**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.

**7. 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.

**8. Reports relating to accidents involving school personnel**.

Reports relating to accidents involving school personnel or occurring on school property shall 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. These reports shall be stored securely in the Secretary's Office and held for the appropriate time.

## Length of time that information will be kept on file

In general personal data shall not be kept for any longer than is reasonably necessary to fulfil the function for which it was first recorded.
Relevant information in student files shall normally be kept for a period of five years after each particular year group has completed Leaving Certificate.
Information which might be pertinent to an allegation of abuse will be retained indefinitely.
Relevant information in staff files shall normally be kept for a period of one year after the staff member has ceased to work in the school. Information which may be of importance in some way or other may be retained indefinitely.
Tax and Pay Records will be kept indefinitely.

## STATUTORY REQUIREMENTS

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 1997 | 3 years |
| Employment Equality Act | 1 years |
| Minimum Wage | 3 years |
| Health and Safety | 10 years |
| Maternity Leave | 1 years |
| Adoptive Leave | 1 years |
| Carer's Leave | 3 years |
| Parental Leave | 8 years |
| Unfair Dismissals | 1 years |

| | |
|---|---|
| Redundancy Payments | 6 months |
| Collective Redundancies | 3 years |

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.

Approved by the Board of Management: May 2014

**Appendix 1**

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

Ballymakenny College is committed to adhere to the provisions of the Data Protection Acts 1988 and 2003, and in 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)**

## 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).