Dualgais scoileanna i leith cosaint sonraí

Aisling Cormican

Associate

Education Unit

Mason Hayes & Curran

21 November 2014

MHC.ie

Dublin
South Bank House
Barrow Street
Dublin 4
Ireland

t +353 1 614 5000
e dublin@mhc.ie

London
1 Cornhill
London
EC3V 3ND
United Kingdom

t +44 20 3178 3366
e london@mhc.ie

New York
1450 Broadway
39th Floor, New York
NY 10018
USA

t +1 646 862 2028
e newyork@mhc.ie

The purpose of data protection law is to protect the privacy of data subjects who provide their personal data to data controllers. The Data Protection Acts 1988 and 2003 ("the Data Protection Acts") govern the rights of individuals who provide personal data to organisations. The Acts also impose stringent responsibilities on those persons holding or processing personal data.

Data Protection is a detailed and at times complex area of law which alone could easily fill a day's seminar. Recently, a new website for schools, www.dataprotectionschools.ie was launched in conjunction with a number of school management bodies. Although the website is useful, and marks the first real guidance for schools on this topic, it does contain a very large amount of information which, anyone unfamiliar with the concept of data protection, could find overwhelming.

Instead, our discussion will focus on the essential data protection issues which arise for schools on a regular basis. By their nature, schools hold personal data relating to a variety of individuals including students, employees, parents, volunteers, former students, members of the Board of Management, and so on. However, today we will largely focus on the data protection issues relating to students and employees.

Before we address some of the provisions of the Data Protection Acts and how they apply to the education sector, it is first useful to look at some of the definitions contained in Section 1 of the Acts.

1. Key definitions

- A ***data controller*** is the individual or legal person who controls and is responsible for the keeping and use of personal information on computer or structured manual files. In schools, Boards of Management are deemed to be data controllers for the purpose of the Data Protection Acts. On a day to day basis the keeping and use of personal information is carried out by employees of the Board; namely the principal, school secretary and teachers.

- ***Data*** includes any automated data held on a computer or recorded for the purpose of being held at a later date on a computer. It also includes 'manual data' comprising of any information kept as part of a 'relevant filing system'. This is defined as any set or file of information, which while not computerised, is structured by reference to individuals so that specific information relating to a particular individual is readily accessible.

- ***Personal data*** means data relating to a living individual who is or can be identified either from the data itself or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This could include manual data recorded as part of a relevant filing system, computer files, emails, biometric scans and CCTV footage, which I will address in more detail below. In principle, the definition covers any information on an identifiable, living individual, *provided it personally relates to them*.

  For instance, the information contained on a CV or on an enrolment application will contain information which personally relates to a student and his/her parents and in some instances, his/her siblings. Another example could be an application made by a principal to the SENO for special needs supports. Such documentation would obviously contain medical information which would personally relate to the student.

- In some instances what constitutes personal data may not be clear cut. The mere mention of an individual in a document does not necessarily mean that the document contains personal information relating to them. Take for instance the fact that an individual is documented in the minutes as having attended a Board of Management meeting. Unless discussion about this individual is documented in the minutes, his/her mere presence at the meeting may not amount to personal data relating to them.

- Similarly, a letter written by a teacher to a parent about a student's progress, may not necessarily contain personal data relating to the teacher if his/her name or title is simply recorded at the end of the letter.

- On the other hand, a multiple choice English quiz on Irish poets may not contain much, if any, personal data relating to an individual student. In contrast, an aptitude test could contain personal information relating to a student. Continuing with this line of thought,

MASON HAYES & CURRAN

while the Data Protection Acts does provides a right for a student to request the *results* of an exam, this does not automatically extend to the *scripts* that were submitted for the exam.

- ***Sensitive Personal Data*** is a special category of data which is prescribed additional protection under the Data Protection Acts. This category of data is defined as personal data which reveals information about racial or ethnic origin, health, political opinions, religious beliefs or trade union membership. As such, this category of personal data is particularly relevant to schools in the context of its employees and students. Sensitive personal data would also include information about the commission of an offence or an alleged offence. I will address this in more detail when discussing Garda Vetting.

- When obtaining and processing sensitive personal data, at least one of a number of conditions set out in section 2(B) of the Data Protection Acts must be met. The most relevant conditions for schools include the following:

    - Consent explicitly given; and/or
    - The obtaining/processing of such information is necessary for the performance of a function conferred on a person by or under an enactment;
    - The processing is necessary for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

Arguably, the obtaining and processing of this type of sensitive personal data relating to students is necessary for the school to perform its functions under the Education Act, 1998 and other enactments. For instance, sensitive personal data obtained in order to make a child protection referral to the HSE would be necessary for the performance conferred on a principal in his/her role as a DLP and as part of his/her functions under Section 23 the Education Act, 1998.

Therefore, in the majority of cases the holding and processing of sensitive personal data will be justified in order for the school to carry out its functions under various enactments including the Education Act, 1998. As an additional measure, schools could request that, on enrolment, consent is sought from parents for the school to obtain and process sensitive personal data.

MASON HAYES & CURRAN

2. Responsibilities of a data controller

There are eight fundamental obligations that a data controller must observe in data protection, some of which are worth some reflection. These are as follows:

- **Obtain and process information fairly;**

  One example of this principle is the necessity to seek parental consent to publish photographs of students on schools' websites or in other material.

- **Keep it only for one or more specified, explicit and lawful purposes;**

  This obligation is relatively self-explanatory. For instance, schools hold personal information relating to students in order to provide them with an appropriate education, to comply with legislative requirements and to ensure that eligible students can avail of supports. In the case of employees, the Board of Management, as an employer, is required by law to hold certain details relating to employees, some of which are documented in this paper.

- **Use and disclose it only in ways compatible with these purposes;**

  In other words, do not use the personal data for some other purpose – such as using parents' contact details to organise a fundraiser for the local football pitch.

- **Keep it safe and secure;**

  What is an appropriate standard of security will depend upon the resources of the data controller and the sensitivity of the data in question. This is particularly the case when you are holding personal data and sensitive personal data relating to minors. At a minimum, you should ensure that access to student and employee records is on a "need to know basis" only; computer systems are password protected; all waste papers, print-outs etc. are disposed of carefully. It may also be necessary to restrict access to the school office.

- **Keep it accurate, complete and up to date;**
- **Ensure that it is adequate, relevant and not excessive;**

MASON HAYES & CURRAN

In the case of records held in connection with a complaint of bullying against a student, obviously the records should be adequate for the purpose of your investigation into the complaint, relevant to the investigation itself and not excessive. For instance, it may not be relevant to document in detail, a child's family circumstances, or details relating to a parent's employment status, unless it was in some way connected with the bullying complaint.

- **Retain it for no longer than necessary for the purpose or purposes;**
- **Give a copy of his/her personal data to an individual, on request.**

I will address retention and data access requests in more detail below. A well drafted data protection policy should address the majority of these obligations for school, provided the policy is adhered to by the Board of Management and relevant members of staff.

3. Retention of data

As stated above, personal data should only be stored for no longer than is necessary. However, a Board of Management is required by law, to retain certain data relating to its employees. The question also arises as to whether the Board should retain records of former students, particularly in the context of potential litigation.

Academic records

Requests are regularly made of schools for academic results many years after students have left the school. For this reason, many schools retain students' academic results for a considerable period of time, for instance until students would be expected to have completed second or third level education. This would appear to satisfy the requirement not to store personal data for longer than necessary when there is some likelihood that former students will request such information. It is reasonable to have a policy that such information will be retained for a finite period of time.

Student files

Retention of personal data becomes more complex if the school wishes to retain all the documentation which comprises a "student's file" for an extended or an indefinite period of time after the student has graduated. Arguably, the original purpose for retaining the data (educating the student) no longer exists. I loosely refer to the term ‘student file’ because there is no definitive list of documents which should be included in such a file. Aside from the regular school reports, enrolment documentation, correspondence with parents, standardised tests and so on, every file will be slightly different.

In the context of potential litigation, particularly in respect of former industrial schools, which litigation often occurs many years after the alleged event, the school may wish to retain such data in the defence of proceedings taken against the school by former students. However, even if the school decided to retain its records in contemplation of possible litigation, it is difficult, if not impossible, to put a definitive limit on the length of time the records should be retained. As mentioned above, personal data relating to student should only be retained for its purpose (ie. educating the students) and stored for no longer than necessary. The Data Protection Commissioner has taken a strict approach to the retention of personal data solely on the apprehension of possible litigation on the basis that this retention is not ‘evidence based’ and because the data is being retained for a different purpose than what was originally intended.

For completeness, I should also say that, health and safety legislation requires organisations including schools, to retain reports of accidents and dangerous occurrences (which could concern both students and employees) for a period of 7 years.

What to do?

Schools could consider taking a proactive approach to these issues. For instance, on enrolment, the school could inform parents that it will retain students’ files after graduation until they reach a certain age. Academic results, which are more commonly requested, could be retained for a longer period.

There may of course be some other relevant reasons why such records are maintained, for instance, in order to maintain alumni records. Where possible, all reasons should be incorporated into the school’s statement on data protection.

Employees

Somewhat confusingly, employers are required to adhere to different retention periods, depending on the particular piece of legislation. I have summarised below the most important of the current retention periods. Bear in mind that this is only a summary of the current law, which may change in the future.

The National Minimum Wage Act 2000 requires an employer to keep such records as are necessary to show that the employees are being paid at least the national minimum wage. Under the Act these records should be retained for at least three years from the date of creation.

The Organisation of Working Time Act, 1997, which governs working time and statutory leave entitlements, requires that records of weekly working hours (including annual leave and public holidays), the name and address of each employee, the employee's PPS number and a brief statement of his or her duties is maintained. Working hours may be recorded manually in a statutory prescribed format or on a computerised clock in system. These records are required to be maintained for a period of 3 years.

In the case of employment contracts, the Terms of Employment (Information) Act requires that an employee's terms and conditions be maintained for the duration of their employment. While there is no obligation to retain a record of the contract after the employment has concluded, a civil claim for 'breach of contract' can be brought for up to six years from the date of breach. For this reason, it would be prudent to retain contracts of employment for at least 7 years from the date of the conclusion of the contract, to allow for claims which might be commenced towards the end of this limitation period.

The Parental Leave Acts 1998 and 2006 require an employer to retain a record of any parental or force majeure leave taken by employees, including the dates upon which the employee was on such leave. These records should be retained for 8 years.

Records of tax payments must be retained for a period of 6 years in accordance with the accounting requirements under the Companies Acts and the Taxes Consolidation Act, 1997.

Finally, as referred to above, health and safety legislation require that reports of accidents and dangerous occurrences (which could concern both students and employees) should be retained for 7 years.

4. Data Access Requests

Under Section 4 of the Data Protection Acts, any individual (including employees, former employees, students, former students and parents) is entitled to request a copy of any information personally relating to them which is kept on computer or on a structured filing system. Bear in mind that a subject access request must be responded to within 40 days of receipt.

All data access requests should be dealt with in the same way.

1. Review the terms of the data access request to establish what information is within the scope of the request.

   Often subject access requests can be very broad in scope. I have included some recent (redacted!) examples in this regard. If an employee requests "all personal data relating to their employment", this would include all information personally relating to the employee which is held on computer or stored in a structured filing system and which is readily accessible. This may include an employee's contract of employment, correspondence, minutes of meetings of the Board of Management in which the employee was discussed.

2. Collate and categorise all of the data held by the data controller which personally relates to the individual.

   We are often asked whether a teacher's or principal's notes relating to an individual should be included in a data access request. This very much depends on the facts of the case. Arguably, if the note was jotted down in a copy book or A4 pad along with a whole range of unrelated information, then such a note could not be said to form part of a relevant, structured filing system. On the other hand, if the note formed part of a file relating to a student or employees, the case could be made that it does form part of a 'structured filing system'.

   Often principals keep information relating to the provision of education supports for children with special education needs in one particular file. We would take the view that this information is 'readily accessible' and if covered by the scope of the data access request, should be included.

One query which often arises is whether data recorded in Irish should be translated into English. This arises from the fact that data controllers are required to provide a copy of what constitutes personal data in 'intelligible form'. We take the view that if students are taught through Irish, it is reasonable to expect that the school will hold personal data relating to staff and students in Irish! Rather than translate the documents (which could be a time consuming exercise), a description in English of the records held could be provided to the data subject.

3. Identify whether certain information should be withheld or redacted.

   There are a limited number of exemptions under the Data Protection Acts. However, it is important to be aware that if personal information is not captured by one of the exemptions, it <u>must</u> be included. I set out below some of the key exemptions which may apply to schools:

   - Information relating to third parties. As a data controller, the school should not disclose personal data relating to other individuals (such as other students or parents). If the redaction of the third party's details could conceal that person's identity, then the document should be redacted.

   - An opinion given in confidence. This exemption would only apply in cases where the opinion was only given on the strict understanding that it was to be treated as confidential.

   - Legally privileged information. Generally, all documents prepared in contemplation of litigation or providing legal advice are legally privileged.

4. Redact any portions of the data which do not personally relate to the individual. If, for instance, a teacher has made a data access request, and the school has retained letters of complaint made against her, she would only be entitled to the extracts of such letters which personally relate to her. Information which does not personally relate to her should be redacted.

5. Redact information relating to third parties (such as other students and parents).

6. Having completed all of the above tasks, you should now be in a position to copy all of the information forming part of the data access request. We recommend that you also retain a copy of what is sent to the individual, along with a third copy of all the personal information relating to the individual, which includes the redacted data or data has been withheld, in the event that the individual queries what he or she is given.

7. Draft a cover letter to enclose with the information to be sent to the individual which states the following:

   - Confirmation that the school holds data which personally relates to him/her;
   - The categories of data held by the school
   - The purpose/s for holding/processing such data
   - The source of the data. For instance, data generated in the course of his/her employment or in the case of a student, generated in the course of their attendance at school;
   - The identities or categories of recipients to whom the data may be disclosed. For instance, to the Department of Education and Skills or the Child and Family Agency.
   - That the individual has an entitlement to complain to the Data Protection Commissioner.

A word on the Data Protection Commissioner

Each Member State of the EU has a dedicated regulator responsible for enforcing data protection law. The Irish Data Protection Commissioner, who is the regulator in this jurisdiction, has a range of enforcement powers including powers of investigation, the power to issue enforcement notices directing the taking of certain actions (such as the disclosure of certain data) and the power to prosecute offences. The Commissioner has been vocal about his priority to improve the general standards of data protection in Ireland and the necessity for organisations to respect the privacy rights of individuals.

Individuals who are unsatisfied with the response they have received from data controllers can make a formal complaint to the Office of the Data Protection Commissioner who may investigate the matter. Most complaints are resolved without recourse to litigation or a formal

MASON HAYES & CURRAN

decision from the Commissioner, provided of course that the data controller makes genuine efforts to resolve the complaint.

CCTV

CCTV systems which are capable of recording identifying features are subject to the provisions of the Data Protection Acts. The school will need to carefully justify the obtaining and use of personal data by means of CCTV.

If it is the case that CCTV is only used to monitor the security of the school premises, then the footage cannot be used for any other purpose – such as monitoring employees or students. The Data Protection Commissioner has commented that the use of CCTV in circumstances other than security, for instance to monitor employees, students etc., can be more difficult to justify. At a minimum, any person monitored on CCTV is entitled to know that they are being monitored.

Therefore, we recommend that the school puts in place a policy for CCTV such that all individuals who attend the school are aware of its purpose and the reasons why the Board deemed it necessary to install a CCTV system. This could be achieved by placing a sign at the entrance of the school in addition to notifying all parents before the system is installed.

Where schools have engaged security firms to manage and operate the cameras and footage on their behalf, such firms are deemed to be “data processors” for the purpose of the Data Protection Acts and are required to have strict security measures in place. We recommend that Boards of Management carefully review the terms of their contracts with such firms in order to be satisfied that there are adequate security measures in place to protect the footage.

If the CCTV is capable of identifying individuals, then such data may be subject to an access request under section 4 of the Data Protection Acts. Individuals who make such requests are required to provide a timeframe of the recording being sought – for instance specific times and dates of when they believe they were recorded.

Bear in mind that the Board, as the data controller, is required to protect personal data relating to third parties. Therefore, any footage the subject of a data access request will have to be edited such that images of third parties are not disclosed. Alternatively, the consent of the third parties to release unedited footage could be sought.

Garda Vetting

The law relating to Garda vetting is an area which could warrant an entirely separate seminar but it is worth highlighting in this discussion how personal data relating to Garda vetting should be treated by schools.

As you would be aware, an employee or volunteer undergoing Garda vetting gives permission to An Garda Siochana to disclose details of all prosecutions and/or convictions held on record. The disclosure of such information allows schools assess the suitability of persons who would have unsupervised contact with minors. This information constitutes sensitive personal data and as such, cannot be processed or used for any other purpose. Careful measures should also be put in place to ensure that Garda vetting disclosures are kept secure.

On the matter of retention, the Data Protection Commissioner has recommended that Garda vetting disclosures are deleted one year after they are received, except in exceptional circumstances. In the case of issues or complaints arising in the future, the reference number and date of disclosure can be retained such that the principal or Board can follow up with the Garda Vetting Unit, if required.

Key Points:

- Prepare a data protection policy which identifies the purpose for which personal data relating to students is held by the school, and if possible, set out the school's position on the retention of students' files.

- On enrolment, inform parents that the school will hold personal data and sensitive personal data relating to students.

- Ensure that all members of staff, particularly those fulfilling administration functions, are aware of and comply with the measures put in place to keep personal data secure.

- When dealing with data access requests carefully review the *scope* of the request to ensure you have gathered all of the relevant data.

- Ask yourself does the data or part of the data *personally relate* to the individual who made the request?

- Ensure that personal information relating to third parties is not disclosed.

- If the school has CCTV in place, ensure that prominent signs are in place stating the purpose of the CCTV. Ensure that the footage, which should not be retained indefinitely, is capable of being edited such that the school can comply with any data access request.