Data Protection for the Guidance Counsellor

Compliant Data Management

Hugh Jones

Data Protection Specialist

Sytorus Data Protection Consultancy

Published by the National Centre for Guidance in Education (NCGE) as an article for the School Guidance Handbook

Contents

Summary

The role of the Guidance Counsellor has been an essential element in providing students and job seekers with professional, objective advice on their strengths, abilities and aptitudes.

As such, the role necessarily involves the processing of personal and often highly confidential information regarding people of all ages. In that context, the activities of the Guidance Counsellor must be compliant with the Irish Data Protection legislation.

This article offers a brief overview of the legislation, as well as setting the day-to-day activities of Guidance Counsellors within that context. The article considers the data being used by the Guidance Counsellor, the particular challenges of working with minors, and the differences between those working as employees of schools or colleges, and those operating as self-employed professionals.

Throughout, we try to offer pragmatic suggestions on how to manage personal data in a manner that is both accessible and relevant for the professional Guidance Counsellor.

Keywords

Data Protection, The Data Protection Acts, Compliance, Data Controller, Data Processor, Data Subject, Data Protection Commissioner, Enforcement, Sensitive Personal Data.

Introduction

This document proposes to provide a brief outline of the Irish Data Protection legislation, with particular reference to the processing requirements of a school-based Guidance Counsellor. The article will consider the obligation to comply with the eight Data Protection Rules, the Rights enjoyed by the Data Subjects under the legislation, and the enforcement powers of the Office of the Data Protection Commissioner.

The role of a Guidance Counsellor has particular relevance in this context – the majority of individuals whose personal data the Guidance Counsellor acquires and processes are minors (under 18), and parental consent will be required in order to properly fulfil this role.

The Irish Data Protection Legislation

There are two Acts in Irish legislation which specifically cover the obligations, rights and enforcement structures around the protection of personal data and its use for commercial and administrative purposes:

- The 1988 Data Protection Act (the Principle Act) and
- The 2003 Data Protection (Amendment) Act.

The legislation protects personal data held electronically (automated data) or in paper form (manual data), as long as it is held in an organised, indexed format (a relevant filing system).

Responsibility for compliance

The primary responsibility for compliance rests with the Data Contoller, in this context the school or college, and then by extension to Data Processors, i.e. any third-party organisation providing professional services to the Controller. This latter group involves Guidance Counsellors, IT support organisations, school nurses, etc.

Definitions

Personal Data

Personal data is data by which a living individual can be identified, either directly (name and address, etc.) or indirectly (student id. number, passport number, reference number, etc.). Personal data can include school administration records, aptitude and psychometric test results, video and CCTV footage, guidance notes, extended family information, special needs requirements, third-party references, exam results, photographs, etc.

Age of Majority

There is no minimum or maximum age at which this legislation applies. The only defining criterion is that the personal data must relate to a 'living individual'. [The same criterion applies to the protection provided by libel and defamation legislation.]
The protection of the legislation applies to people of all ages, including children, teens and young adults, as long as their personal data is processed within the jurisdiction of the Republic of Ireland.

Recommendation: Where a school is processing the data of under-age children (typically understood as under 18 years of age), it is recommended to inform the child's parents or guardians of such processing.
Where a school or Guidance Counsellor is processing the data of students who are over 18 years of age, such students should be treated as adults and the processing of their personal data should be explained to them directly.

A Guidance Counsellor will often engage with third party organisations on behalf of his/her students (e.g. potential future employers, universities, social workers, etc.); the Guidance Counsellor should have the consent of both the student and the student's parents or guardians before any personal data is disclosed.

Sensitive Personal Data
The Data Protection Acts recognise that certain data is particularly susceptible to discrimination or prejudice, and deserves an additional level of protection – this includes data on an individual's racial or ethnic identity, their political, religious or ideological beliefs, their sexual orientation and any information on an individual's mental or physical health, etc. This category would also cover the management of information where a student has a criminal or juvenile criminal record.

Where such data is held by a school, the school should be particularly careful regarding its processing. For example, a Guidance Counsellor may be required to notify a prospective employer of a student's medical allergies, criminal record or religious affiliation. This is, of course, permissible, but only as long as it is relevant to the circumstances of the role or work placement.

Characters defined in the Legislation
The Acts identify three main characters in relation to the management of personal data:

- The **Data Subject** – the living individual to whom the data relates. For the most part, the Guidance Counsellor will gather data on the students for whom he or she will be providing guidance counselling, but they will also have contact details for employers and others who support their guidance activities;
- The **Data Controller** – the organisation responsible for gathering, processing and storing the data – in the context of this document, the school which the student attends is the Data Controller. Where the Guidance Counsellor is employed by the school, they must comply with the school's data protection policy (assuming they have one) and obligations, within the terms of their contract of employment.
- The **Data Processor** – any third party organisation contracted by the school, in order to perform a specific task or function in which personal data is processed (e.g. a specialist service provider, a self-employed Guidance Counsellor, etc.). Since there is no employment contract in such circumstances, the law requires that there must be a formal, contractual arrangement in place between the school (as Data Controller) and the self-employed Guidance Counsellor before any personal data is shared. The contract must make specific reference to the data management obligations of the Guidance Counsellor's role. Once an appropriate Data Processor contract is in place, any

data protection obligations carried by the Data Controller extend to the Data Processor for the duration of the engagement.

As the Data Controller, the school is primarily responsible for the gathering, storage, retention and disclosure of their students' data. The school is therefore the primary entity to which the Data Protection obligations apply. However, once engaged or employed by the school, the Guidance Counsellor also carries the same data management obligations.

Recommendation: The Guidance Counsellor should prepare a short narrative explaining their purpose for gathering a student's personal data. This could include reference to the school for which they work, the range of data that they will require, and the fact that they may share the data with employers, prospective employers and other organisations on behalf of their students.
We also recommend that the Guidance Counsellor provide this explanation both to the students with whom they work, and the students' parents and/or guardians.

The Data Protection legislation does not provide a template for such a narrative, but there is an outline in the appendix to this article which offers some suggestions regarding clauses to include in the contract.

The Data Protection Rules

As the Data Controller, the school management and its entire staff must comply with eight data protection rules set out in the legislation.

Where the Guidance Counsellor is an employee of the school, she/he must primarily comply with the school's policies. Later in this article, we will look at compliance obligations where the Guidance Counsellor is a self-employed, third-party, engaged by the school under contract.

1. The data must be **obtained fairly**, where possible with the consent and awareness of the Data Subject, and where relevant, their parents or guardians.

    a. **Recommendation:** Where the school does not already have one, we recommend that the school drafts a Data Protection Policy outlining the school's commitment to acquiring, holding, processing and storing the personal data in compliance with the legislation. Please see Appendix I of this article for suggestions on the content of a Data Protection Policy.

    b. **Recommendation:** Since the majority of students with whom the Guidance Counsellor is working are under 18 years of age, the school should communicate with their parents or guardians at the start of each school year, explaining the fact that the students' data will be acquired and processed for a number of purposes, consistent with the school's activities.

    c. **Recommendation:** The Guidance Counsellor should explain clearly, to both students and their parents or guardians, the fact that their

personal data will be captured in the course of the Guidance Counsellor's work with them, that the Counsellor may be required to disclose their data to others, and that the data will be held in compliance with the Irish DP legislation.

2. The data can only be obtained for a **specific purpose or purposes** – the Data Controller must be able to justify acquiring, storing, processing and using the data.

    a. **Recommendation:** Consider the various purposes for which the school requires student data, and the minimum set of data required to fulfil these purposes. The school should then limit acquisition of personal data to this data set. School staff should resist the temptation to gather additional personal data – mobile numbers, e-mail addresses, etc., unless the data is specifically required.

3. Processing of the data must be **compatible** with the specific purpose or purposes. The Guidance Counsellor must confine the processing of the personal data to the purpose or purposes for which the data was acquired.

4. The data must be kept **safe and secure at all times during processing**, making appropriate use of available technology – this applies equally to manual and automated data. The school has a duty of care to ensure that the data gathered is held safely and securely for the duration that it is retained. The school should bear in mind that the notes taken during guidance sessions are particularly confidential, and may qualify as Sensitive Personal Data (defined above). As such, they deserve an additional level of care and protection under the legislation.

    There is often a risk that the school might be tempted to sacrifice security for convenience – e.g. allowing all staff to access student records, or enabling staff to access the school network remotely, in order to be able to work from home, or outside normal school hours. While these solutions might allow more efficient processing of data, they increase the risk of data loss, data leakage or inappropriate or unauthorised access to student records.

    a. **Recommendation:** If the school does not already have one, we recommend introducing a policy of encrypting all mobile computing and data storage equipment (USB keys, external drives, smart phones, laptops, etc.).

    b. **Recommendation:** Access to manual and electronic records should be strictly limited, and only those with a particular need or authorisation to do so should be able to see and modify this data.

    c. **Recommendation:** Ideally, student data should be stored centrally by the school so that access can be limited and its use can be controlled. Again, this applies equally to manual and electronic records.

5. The data must be kept as **accurate and up-to-date** as necessary by the school and its staff. Obviously, it is in the school's own interest to ensure that their data is current and accurate, in order to be able to provide the best support and advice possible to the students in their care.

    a. **Recommendation:** If the school is holding data on students over a period of several years, the school management should introduce some mechanism to make sure that the data are regularly checked for accuracy and currency, and are updated accordingly once the school are informed of changes.

    b. **Note:** each Data Subject has a right, under the legislation, to request the correction of any inaccurate data relating to them which the school may hold.

6. Processing and disclosure of personal data should be **adequate, relevant and not excessive**, based on the specific purpose(s);

    a. **Recommendation:** In the course of the Guidance Counsellor's work with the students, they will be expected to disclose their information to other organisations, e.g. prospective employers, work experience assignments, etc. The Guidance Counsellor should only disclose the minimum of student data required by these parties, in order to fulfil their obligations to their students.
    b. **Recommendation:** Under the Irish Data Protection Acts, neither organisations nor parents have an automatic right of access to data relating to the students. The management of school and student records is determined by a range of Irish legislation. This should be borne in mind when considering requests for data sharing, disclosure, the acquisition of student data, etc. As with any other organisation, the school should be aware of the legal obligations which are relevant for their management of personal data, and strive to comply with these obligations.
    c. **Recommendation:** Any request for access to a student's personal data should be taken on its merits, and we recommend that the school requires that any request for personal information on a student should be submitted in writing, with a clear explanation for the basis of the request, and should be considered by the school management before a decision is taken regarding a response.

7. Personal data **should only be kept for as long as necessary**, usually determined by the specific purpose mentioned in (2) above, as well as obligations under other Irish legislation. Current legislation sets a range of retention obligations with which the school must be familiar, and most records relating to student services must be retained for a minimum of seven years after the student has left the school. This rule applies equally to data held in automated (computerised) and manual format (paper records).

    a. **Recommendation:** The school should only keep a student's data for the duration of the period that the school is providing guidance

services to that student plus seven years. Thereafter, student records and correspondence should be reduced to the bare minimum which the school needs to retain for its historical records. As set out in (4) above, this data should be stored in a secure location.

b. **Recommendation:** Preferably, as much student data as possible should be anonymised, and any unnecessary copies destroyed.

8. **A copy of their personal data** must be made available to the Data Subject on request.

    a. **Recommendation:** School staff must ensure that student data is held and stored in an efficient and retrievable manner. On receipt of a valid access request, the school needs to be able to respond in a timely manner, but no longer than 40 calendar days from receipt of the request.

The obligations of the self-employed Guidance Counsellor

The eight rules outlined above apply primarily to the school as the Data Controller. In turn, the school employees must comply with the obligations set out by the legislation. Where a Guidance Counsellor is not an employee of the school, but is engaged on contract for a fixed period of time, this obligation changes slightly. As a separate legal entity, the Guidance Counsellor is a Data Controller in their own right, with direct obligations under the legislation. As a contractor, they must have a formal contract in place with the school before they can process personal data of the school's students.

Although the Data Protection legislation requires this contract to be in place, there is no provision within the legislation setting out the content or structure of the contract.

It is generally accepted that the Data Processor contract, agreed between the Controller and Processor, should set out the scope and range of activities which the Guidance Counsellor is expected to perform in the fulfilment of his or her duties at the school. It is critically important that the contractor confines their subsequent processing of student data to the terms set out in the contract. To do otherwise (to process data in a manner not permitted in the contract) would be to risk a breach of contract, as well as a breach of the Data Protection legislation.

The Data Subject Rights

Regardless of age, the Data Subject enjoys certain rights under the legislation, including the one just mentioned – the right of access to a copy of any data relating to them, which is held either by the Data Controller or by the Data Processor.

In order to request a copy of their data, the Data Subject must submit a request in writing, providing sufficient identification and pay a maximum fee of €6.35. Many organisations do not even charge this fee, and a decision to do so is at the discretion of the Data Controller.

Any other costs involved in locating, copying, packaging and posting the data must be met by the Data Controller.

This obligation relates to both manual and electronic data. Once a valid request is received, the school must respond as quickly as possible, but in any case, within 40 calendar days of receipt of the request.

Data Management Policies

Recommendation: If a school does not already have them, school management should ensure that the school has, at a minimum:

- a Data Protection Policy
- a Data Protection Statement posted on their web-site or hand-book
- a Data Retention and Destruction Policy, and
- a Subject Access Request Procedure.

Guidelines for the Data Protection Policy are outlined in the Appendix I at the end of this article.

The Data Retention Policy outlines how long certain personal data is held, and an associated Data Destruction Policy, should describe how the various categories of data are destroyed once they are no longer required.

Various pieces of legislation set the required retention schedule for data, e.g. the Education legislation for student records, C.V's, qualifications, exam results, etc.

The Subject Access Request procedure should outline for school management and staff the approach to be adopted for responding to a request by a Data Subject for a copy of their (the Subject's) personal data. The objective of the Procedure is to ensure the most efficient process possible in order to gather data and prepare a compliant, comprehensive and timely response to the Data Subject.

Powers of the DP Commissioner

The Office of the Data Protection Commissioner is the primary enforcement power for this legislation, and the Office of the Commissioner maintains a valuable, public information service through its web-site at http//:www.DataProtection.ie.
The Commissioner's Office is based in Portarlington, Co. Laois, and the current Commissioner is Ms. Helen Dixon, who took up the role in October, 2014. The term of office is five years.

In the event of disputes over processing of personal data, the Office of the Commissioner usually tries to negotiate an amicable settlement between a Data Subject and a Data Controller or Processor. However, if he feels that the case merits a stronger approach, his Office can issue a formal order requiring certain changes to data processing until procedures have been corrected or until the Controller or Processor is fully compliant with the legislation.

Offences under the Irish legislation are punishable by fines of up to €3,000 per offence for a summary prosecution (individual or low severity) and up to €5,000 per offence where the breach involves the use of electronic media, such as unsolicited e-mail, texting or unlawful calls to a person's mobile phone.

Overseas Transfer of Personal Data

Ideally, personal data of students should be processed and stored within the jurisdiction, but will be equally protected anywhere within the 28 member states of the EU, and a limited number of other countries which the EU considers to be 'safe' in data management terms.

If it is necessary to send the data outside this jurisdiction, the school and its staff must take steps to ensure that there will be an adequate level of protection provided to the data in transit and at its destination, before the data is sent.

Conclusion

The Irish Data Protection legislation should be seen as an enabler of, rather than a hindrance to good school and office administration. By being compliant with the Rules, the school and its staff will have a better understanding of the information they hold and process, the accuracy and quality of that data, where and how long it is stored, and how and by whom it is used.

In turn, the decisions made on the basis of such personal information will be of better quality, more relevant, more appropriate and of more benefit to the student to whom the personal data relates.

Further Information:

The Irish Data Protection legislation can be viewed on the web-site of the Office of the Irish Data Protection Commissioner at www.DataProtection.ie.

The Association of Data Protection Officers offers valuable advice and insights on the practical challenges of data managers and users (www.DPO.ie).

Biography – Hugh Jones

Hugh Jones is a certified Data Protection specialist, and a founder and director of Sytorus (www.sytorus.com), a leading Irish data management consultancy.
Hugh can be contacted at Hugh.Jones@Sytorus.com.

Hugh delivers training, provides professional advisory services and is a frequent speaker at Privacy and Data Management events in Ireland and overseas.

As a certified Data Protection practitioner and an experienced project management consultant, Hugh supports organisations striving to achieve and maintain compliance with the Irish and European legislation.

He facilitates projects to design and deploy appropriate policies and procedures in relation to data privacy, data quality and records retention, and conducts regular site audits and process evaluations on behalf of his clients.

.

Appendix I - Guidelines for a Data Protection Policy

While the Irish Data Protection legislation offers no prescriptive set of criteria for a formal Policy, it is possible to infer that an organisation's Policy should contain the following (in no particular order of priority):

- Clear identification of the Organisation itself, including its registered address
- An outline of the category or categories of personal data which the organisation requires for its day-to-day operations
- The purpose or purposes for which the organisation requires such data
- An outline of circumstances where the organisation may engage a third-party service provider in order to process personal data on its behalf
- Reassurance that the organisation is aware of its obligations under the Data Protection legislation, and is committed to comply with such obligations
- Contact details through which a Data Subject can register any data management concerns with the organisation