Data Protection for the Guidance Counsellor

Compliant Data Management

Author: Hugh Jones

Data Protection Specialist

Sytorus Data Protection Consultancy

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.

Introducing a further challenge, in May 2018 the Irish and European Data Protection landscape will change significantly with the introduction of the General Data Protection Regulation – a new set of data management obligations which will take effect across the European region on the same date.

This article offers a brief overview of the Regulation, 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, General Data Protection Regulation, GDPR, Compliance, Data Controller, Data Processor, Data Subject, Data Protection Commissioner, Supervisory Authority, Consent, Enforcement, Sensitive Personal Data.

Introduction

This document offers a brief outline of the Irish Data Protection legislation, including the impending General Data Protection Regulation (GDPR) with particular reference to the processing requirements of a school-based Guidance Counsellor. The article will consider the obligation to comply with the seven Data Protection Principles of the GDPR, as well as the Rights enjoyed by the Data Subjects under the legislation, and the enforcement powers of the Office of the Irish 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.

It should be noted that the GDPR has introduced a further requirement with regard to the age of consent – specifically with regard to setting up 'information society services', e.g. e-mail, social media and mobile phone accounts. In such circumstances, the Irish government has determined that a child aged 14 or older can proceed and request the set-up of such an account at their own discretion. However, where a child is aged 13 or younger, prior parental or guardian approval must be acquired, before such an account can be set up.
In a school context, this would apply where a school or class were planning to set up a WhatsApp group for a particular project, or were offering school e-mail addresses to pupils for assignments and project activities.

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.

These two Acts will be replaced on May 25th, 2018, with a single Regulation, known as the General Data Protection Regulation (or GDPR), which will govern the manner in which personal data is processed across the European region for the foreseeable future.

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 Controller, in this context the school or college, and then by extension with Data Processors, i.e. any third-party organisation or individual providing professional data management 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, but under-13 for certain situations, as outlined previously), 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.

In line with the GDPR, the Irish government has determined that certain processing of personal data relating to children under the age of 13 cannot be conducted without parental approval. As mentioned earlier, this includes the provision of electronic communications accounts. For example, where a school assigns an e-mail account to its pupils to enable submission of home-work, or for collaboration on projects, parental approval must be acquired before accounts can be set up for pupils aged 13 or under.

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 must have the consent of both the student and the student's parents or guardians before any personal data is disclosed.

Special Categories of Data Processing

The Data Protection Regulation recognises 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. In the schools context, the results of standardised ability tests (SAT's) would qualify as an indication of an individual student's mental and academic ability, and would therefore qualify as a special category of processing.

Where such data is held and processed by a school, the school should be particularly careful regarding its use. For example, a Guidance Counsellor may be required to

notify a prospective employer of a student's medical needs, allergies 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 Regulation

The legislation identifies three main characters in relation to the management of personal data:

- The **Data Subject** – the living individual to whom the personal 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.

It is also the responsibility of the Controller to ensure that the appropriate Data Processor Agreement is in place. The GDPR will require that certain specified clauses are included in this contract, covering topics such as the duration of the contract, the subject matter, the categories of personal data being processed, and the security measures in place to protect the confidentiality and integrity of the data.

Recommendation: The Guidance Counsellor must prepare a short narrative explaining their purpose for gathering a student's personal data. This could include reference to the school for whom 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 Regulation 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 Principles of the GDPR

As the Data Controller, the school management and its entire staff must comply with seven data protection principles set out in the new Regulation. These are largely consistent with the eight Rules which set the framework for preceding legislation.

Where the Guidance Counsellor is an employee of the school, they 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**, and processing should be conducted in a lawful, open and transparent manner. As with the preceding legislation, processing should ideally be with the consent and awareness of the Data Subject, and where relevant, their parents or guardians. However, it is possible that other lawful conditions exist to justify the processing, even where consent is not available or is being withheld. For example, a school might be obliged, under safeguarding legislation, to notify authorities of concerns regarding the welfare of a student, even where parental consent is not available or not forthcoming.

    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. While a Data Protection Policy is not specifically mandated by the Regulation, it represents good practice and offers a degree of transparency to parents and children alike by setting out clear expectations regarding the intended processing of their personal data.
    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. The school should also provide assurances that the personal data will not be used for other, secondary purposes.
    Many schools seek confirmation of parental consent at the start of first year, and rely on this for the duration of the following 4-5 years of the student's time at the school. Best practice would indicate that this consent should be renewed or reviewed each year at the start of term, to ensure that no substantial change in circumstances has occurred in the intervening year.

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 relevant 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. The school should then set reasonable expectations with both students and parents/guardians regarding the lawful purposes for which the data will be used.

3. The school should only conduct the **minimum range of processing** necessary to achieve the specified, lawful purposes for which the data was acquired. Any processing should be limited to this minimum. School staff should resist the temptation to gather additional personal data – mobile numbers, e-mail addresses, etc., unless the data is specifically required. Subsequent retention and use of the data should also be kept to a minimum – e.g. schools holding onto exam results or SAT test scores indefinitely would appear to breach this Principle.

   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.

   Recommendation: Under the Irish Data Protection Regulations, neither organisations nor parents have an automatic right of access to data relating to the students. While a parent or guardian is entitled to act on behalf of the student, there are circumstances where school management might determine that the disclosure of certain information to a parent or guardian might not be in the student's best interests.

   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.

   a. **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.

4. 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. At least once per year, during registration, the school has an ideal opportunity to check the accuracy and currency of any personal data it holds with regard to its students and their parents, emergency contact details, medical conditions, etc.

    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.

5. 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 (e.g. employment law, tax regulations, health and safety obligations, etc.). 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 or duplicate copies destroyed.

6. 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.

The Regulation requires the Data Controller to implement appropriate technological, organisational and physical solutions in order to protect the confidentiality and integrity of the personal data.

- Technological solutions – password protection on files, limited access to the network, discretion when sending e-mails, 'locking' PC screens when not in use, etc.
- Organisational solutions – limiting the level of access to records based on staff members' roles and responsibilities, etc.
- Physical solutions – locking office doors when rooms are not in use, deploying CCTV on the school grounds, adopting a 'clean desk' policy in all offices, providing lockers to students for the safe storage of their books and documents, etc.

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 IT 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.

7. The Data Controller must implement appropriate solutions to demonstrate its **responsibility and accountability** towards the personal data for which it is responsible.

The GDPR will introduce some obligations which require the school to be able to demonstrate its compliance with the Regulation. These include:

- Data Process Logging – all organisations – Processors as well as Controllers – will need to draft and maintain a description of their main data management processes, based on a set of headers outlined in the GDPR. These include the range and scope of processing, the purpose for the processing, and whether it is being done by the School or by a third party on its behalf;

- Privacy Impact Assessments – the GDPR has introduced the notion of Privacy By Design – i.e. that any project leading to a system or process change which will introduce risk for personal data must include a Privacy Impact Assessment – an evaluation of the anticipated risk as well as a documented report, partly as evidence that the assessment was conducted and also outlining the risk mitigation measures which were undertaken to address the risk;

- Breach Notification Reporting – from May 2018, any perceived breach in the management of personal data will merit a formal notification to the Office of the Irish DP Commissioner – again, Guidance has been provided by the ODPC, and is available from their web-site at www.DataProtection.ie;

- Data Protection Officer (DPO) – any organisation meeting certain criteria must appoint a DPO as the 'go to' person for guidance on the day-to-day management of personal data within the organisation, as well as to be the primary point of contact for external parties, the Regulator, etc.

- The three mandatory criteria are:

    - Where an organisation is a public body or authority
    - Where the organisation conducts systematic surveillance of members of the public (e.g. a city council deploying a CCTV monitoring system), or
    - Where the organisation regularly conducts special categories of processing, such as with information on medical conditions, ethnic identity, religious affiliation, etc.

- Even where organisations do not meet the mandatory criteria, we recommend that, as good practice, a member of staff should receive formal training with regard to the GDPR, in order to be able to explain and shape the organisation's data management practices.

The obligations of the self-employed Guidance Counsellor

The seven principles 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 contractor, they must have a formal contract in place with the school before they can process personal data of the school's students. For example, a test publisher which facilitates the administration and hosting of test results on behalf of a school would be a clear example of a Data Processor, for which the school would need to have a formal, written contract in place with the publisher.

In a change from previous legislation, the GDPR sets out twelve clauses which must be referenced in any such contract between the school (as Data Controller) and its service providers and contractors (the Data Processors). These include:

- The subject-matter of the intended processing
- The duration of the processing

- The nature and purpose of the processing
- The type(s) of personal data involved – e.g. whether 'ordinary' or Sensitive
- The categories of data subjects involved – employees, customers, donors, marketing 'leads', etc.
- The obligations and rights of the Controller, particularly where the Controller sets out parameters for processing, or imposes constraints on the data management activities of the Processor.

In addition, the contract must provide clauses regarding the following responsibilities of the Processor, including:

- That the Processor only processes the personal data based on documented instructions from the Controller;
- That the Processor ensures that persons authorised by the Processor to process the personal data have committed themselves to protecting the confidentiality of that data;
- That the Processor takes all appropriate measures required to ensure the security of the personal data;
- That the Processor respects the preferences of the Data Controller with regard to engaging another processor or sub-contractor;
- That the Processor assists the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation in responding to requests relating to a data subject's rights;
- That the Processor assists the controller in ensuring compliance with the obligations regarding data security, in as far as possible;
- That, at the choice of the Controller, the Processor deletes or returns all the personal data to the controller after the end of the provision of services outlined in the contract;
- That the Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations set out in the Regulation, and allows for and contributes appropriately to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

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 Regulation.

The Data Subject Rights

Regardless of age, the Data Subject enjoys certain rights under the new Regulation, some of which are outlined below. Both the Controller and the Processor have obligations to respond in a timely manner when these rights are invoked by a Data

Subject (whether they are a student, parent, teacher, Guidance Counsellor or member of the public).

Right of Access to one's personal data
In order to request a copy of their data, the Data Subject must submit a request in writing, providing sufficient identification to satisfy the Data Controller as to their identity. In the case of a minor, naturally, their parent or guardian can submit a written request on their behalf. Under previous legislation, it was possible for the school to charge an administrative fee for this service, but under the GDPR, no fee is permitted.

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 30 calendar days (one month) of receipt of the request.

Right to have inaccurate personal data corrected
Where a Data Subject becomes aware that an item of personal data which relates to them is inaccurate or incorrect, they are entitled to provide evidence of the correct detail, and to require the Controller to update the information accordingly.

Right to be forgotten
In certain circumstances, an individual might request to have any personal records which the Controller holds removed or deleted – a right being labelled the 'right to be forgotten'. However, the Controller can retain those records where they can demonstrate a legal or contractual obligation to do so (e.g. there may be a directive from the Dept. of Education and Skills, requiring information on registrations or exam results to be retained for a certain number of years.). On the other hand, a school might initiate standardised ability test at its own discretion, and therefore would be obliged to remove any individual test results at the request of the data subject in question.

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 Irish 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 she feels that the case merits a stronger approach, her 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 have been 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.

Under the GDPR, the 'capped' or maximum value of these administrative fines and penalties will be increased significantly, to €20m or 4% of an organisation's global annual turnover (whichever is the greater value). While it is unlikely that such a huge fine will ever be imposed on an Irish educational institution, the Regulation will nonetheless introduce the provisions by which they become possible.

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.

The Brexit negotiations, currently under way, will not impact this consideration, since the provisions of any final Brexit settlement will not take effect until mid-2020 at the earliest.

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. The fact that the data is being processed outside of the EU jurisdiction should also be mentioned in the school's Privacy Statement, or any material sent to parents in relation to the particular programme or processing.

Conclusion

The Irish Data Protection Regulation, when it comes into force from May 25th, 2018, should be seen as an enabler of, rather than a hindrance to good school and office administration. By being compliant with the seven Principles, 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 Office of the DP Commissioner has provided specific guidance on preparing for the GDPR at a separate web-site location - http://gdprandyou.ie/.

In order to help organisations understand and meet their Data Protection obligations, Sytorus has developed an online tool, Privacy Engine, which can be viewed at www.PrivacyEngine.io.
Demonstrations of the key functionality are available free of charge and without conditions.

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