

The General Data Protection Regulations (GDPR) Handbook

A Guide for IGC members on the legislative and compliant management of personal data Guide for IGC members under GDPR.



Drafted by the IGC with Sytorus Ltd. for members of The Institute of Guidance Counsellors

First draft Sept. 2018, Revised Feb., 2019.



Contents

The purpose of this Handbook

Introduction

Definitions

Principles of Data Protection Legislation

Accountability and Liability

Scenario: Correspondence with Parents, Students or Staff

Scenario: Registration of Students

Scenario: Managing Data Security

Scenario: Breach Management and Notification

Scenario: Requests for Disclosure of Personal Data

Scenario: Appropriate Note-taking

Scenario: Management of Consent

Scenario: Records Retention and Destruction

Scenario: Fund-raising and Promotional Activities

Scenario: Involvement of Third-Party Service Providers

Scenario: Data Processing Activity Logs

Scenario: Use of photos and video images

Scenario: Right of Access Requested by the Data Subject

Responding to Data Subject Rights

Compliance with other Standards and Regulations

Further Information and References

Appendix I - Frequently Asked Questions

THE PURPOSE OF THIS HANDBOOK

The purpose of this handbook is to provide practical guidelines for members of the Institute of Guidance Counsellors (IGC) in order to manage their client's/students' personal data in a compliant manner.

Irish Data Protection legislation recognises the organisation (e.g. school, institute or private practitioner) as the Data Controller, “the legal entity which, alone or with others, determines the processing and use of the personal data”. Staff who are employees of the organisation, who gather and process personal data, are doing so on behalf of the organisation, and must comply with that organisation's data management procedures in order to protect the privacy rights of individuals, to protect the organisation's reputation and, where possible, to avoid breaches of the legislation.

Please note that this Handbook at times makes reference to tasks and responsibilities of school management rather than those of the guidance counsellor themselves. Where such information is present, it is only included to provide background operational advice, context and clarity to IGC members working in these contexts. ***This Handbook should not be seen as providing formal data protection advice to school management.***

Where guidance counsellors are working as self-employed practitioners, they are Data Controllers in their own right. In such circumstances, the obligations and recommendations outlined in this Handbook which relate to the Data Controller will apply to them individually. In this, and in other cases, the term “organisation” shall be used to refer to the various settings within which our members are employed (schools, ETBs, prisons, HEIs, Adult Guidance Services, etc.). For guidance counsellors who are employees of a school/institution, the organisation,

as a distinct legal entity, will be the Data Controller and will determine Data Protection protocols and policy.

Compliance with this national legislation is enforced by the Office of the Irish Data Protection Commission, based in Portarlington, Co. Laois, and will be based on adherence to the seven Principles which form the framework for the General Data Protection Regulation (GDPR), an EU Regulation that replaced the pre-existing DP legislation in May 2018.

Any data management activity involving personal information which is conducted by a Data Controller, or by a Data Processor on their behalf, must comply with the ***seven principles*** of the GDPR from May 2018 onwards. These principles are outlined in subsequent pages.

Compliance with the legislation can be seen from three perspectives:

Personal: The personal data which the organisation processes relating to its students, staff, parents or visitors;

Professional: Within the day-to-day activities of the organisation, the legislation requires that staff manage the personal data in a compliant and appropriate manner;

Reputational: Any breach of the legislation reflects negatively on the credibility and reputation of the organisation, and damages peoples' trust in the institution and its activities. Managing the personal data in a compliant manner reduces the risk of this happening.

INTRODUCTION

In managing their day-to-day activities, most academic institutions collect and use personal data about their staff, clients, students and visitors for a variety of purposes.

Within the context of this Handbook, we will focus on the work typically done by the guidance counsellors within schools, colleges, institutions (“organisations”) in addition to those who work as private practitioners.

In general, the data processing activities undertaken by guidance counsellors in schools will include:

- the administration of individual client/student data, annual registration of school/organisation attendance, and participation in the life of the school campus;
- the gathering of appropriate contact details of parents, guardians and family members who are the primary points of contact in relation to the clients’/students’ education and welfare;
- the disclosure of this personal data to appropriate authorities, governing bodies, national organisations, inspectors and/or officers;
- the administration of a school’s activities (daily assembly, regular staff meetings, multi-agency meetings to discuss performance and welfare issues, team management, appointment of mentors, preparation for events and excursions, award ceremonies, graduations, etc.);
- Notes taken, and information divulged during the course of guidance counselling and welfare-related meetings, appointments and assessments;
- Correspondence with parents and guardians relating to the welfare and performance of students under a school’s care;
- Compliance with statutory obligations (including Garda Vetting, Health and Safety, Child Protection and Safeguarding, annual reports, etc.);
- Information on student welfare incidents which occur on school premises, including individual behaviour, injuries or distress suffered,

- medical diagnosis and treatments, as well as the processing of insurance claims for students injured while participating in school activities;
- Bookings and administration of school premises and facilities, such as function and meeting rooms, classrooms, gym and assembly halls, etc.
- Promotion of a school's social and cultural events

Activities typically undertaken by Guidance Counsellors in contexts other than schools will additionally include the following:

The Irish Data Protection legislation safeguards the privacy rights of individuals of all ages in relation to the processing of their personal data. When organisations gather personal data (data relating to living individuals) for any purpose, they must comply with the obligations of this legislation.

This legislation places responsibilities on those persons or organisations processing personal data, as well as conferring rights on individuals as to how their personal data is managed, and the extent to which they can control and access the information held about them.

DEFINITIONS

The following terms are defined within the legislation:

Defined Term	Definition
"Personal Data"	means data which relate to a living individual who can be identified directly from that data (such as a name and address, contact details or photograph), or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller or Data Processor, such as employee number, PPS number, passport number or vehicle registration number. Personal data extends to data which is capable of directly or indirectly identifying an individual, Including online identifiers, GPS location data and IP addresses, etc.
"Special Categories of Personal Data"	Includes the processing of Personal Data involving an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless appropriate conditions are met.
"Processing"	means performing any operation or set of operations on the personal data, whether by manual or automated means. This includes collecting, organising, storing, altering, disclosing, sharing or adapting such data.
"Data Controller"	means any organisation responsible for the processing of the personal data.
"Data Processor"	means any organisation or individual which processes personal data on behalf of the Data Controller but is not an employee of the Data Controller. This would include any third-party organisation using personal data to help the Controller with direct marketing, fund-raising, student registrations, IT services, data storage, etc.
"Data Subject"	means a living individual who is the subject of the personal data, i.e. the natural person to whom the personal data relates.

PRINCIPLES OF DATA PROTECTION LEGISLATION

Organisations must manage the personal data which they gather based on the following seven Data Protection Principles enshrined in the GDPR, and reinforced under the Irish Data Protection Act (2018):

Principle 1- Lawful, fair and transparent processing: The staff of the organisation must obtain and process personal information fairly, with the clear knowledge and awareness of its students, and in turn, of their parents and/or guardians. As much as possible, the organisation should explain what it plans to do with the data, and be able to justify the processing, if asked.

Principle 2- Purpose Limitation: The organisation must keep the data only for one or more specified and lawful purposes, such as the purposes outlined above. Staff of the organisation should avoid using the data for anything other than these purposes.

Principle 3- Minimisation of Data Processing: The staff of the organisation must only use and disclose the data for the purposes agreed by the organisation, and to the minimum extent necessary in order to achieve those purposes. Typically, this will include school administration, student welfare, correspondence with parents and notifications about upcoming events.

Principle 4- Accuracy and Currency: The organisation must keep the personal data as accurate, complete and up-to-date as possible. The organisation should have procedures that ensure high levels of data accuracy and to ensure that personal data on students and colleagues are kept up-to-date and fit for purpose.

Principle 5 – Limited Retention in a Format which Permits Identification: The personal data should only be retained for as long as necessary in a format which permits the identification of the individual, in order to satisfy the specified purpose(s), or as required by law and should then be anonymised, or verifiably destroyed in an appropriate and secure manner.

Principle 6- Data Security and Integrity - Protection of Individuals' Privacy: At all times while the data is within their care, the staff of the organisation should keep the data safe and secure from unlawful or unauthorised access, disclosure, modification or deletion.

Principle 7- Accountability and Liability: The GDPR requires that the staff of the organisation, and, in turn, associated service providers or Data Processors, should be able to demonstrate their 'culture of compliance' with reference to evidence of embedded processes, data management protocols and governance structures.

In the following section, we will look at different ways in which guidance counsellors can process personal data in their day-to-day activities, while remaining in compliance with the legislation.

ACCOUNTABILITY AND LIABILITY

While the organisation has ultimate responsibility for compliance, all members of staff who collect and process the personal data on behalf of the organisation need to be aware of their responsibilities under the Data Protection legislation. This Handbook is intended to be a guideline to all members of the IGC to ensure that they are aware of their obligations under the legislation.

In certain circumstances, the senior Executive team of the organisation can be held individually liable for breaches of the Data Protection legislation, where a breach is found to have been caused by their direct involvement, negligence or 'connivance'. In the context of Guidance Counselling, this would apply to the Board of Management of the school or institution in which the Guidance Counsellor is employed.

Such liability is currently capped at €50,000 per person.

The organisation should also advise its staff of the appropriate procedures to follow in relation to data acquisition, storage, disclosure and processing.

Where guidance counsellors are self-employed (e.g. working in their own private practice) or are self employed as opposed to being the direct employees of the institution/school in which they work, they are considered to be **Data Controllers**, and carry liability for the personal data which they process during the course of their engagement.

It is critical that self-employed guidance counsellors have a Data Processor Agreement in place with a school/institution, governing their access to and use of confidential personal information during the term of their engagement.

Note:

The following scenarios are intended to provide examples of best practice regarding data management during the typical activities of an *educational institution*. They are meant as general data management guidelines only – the content of this Handbook does not constitute legal advice.

If your administrative or professional activities involve other processing of personal data on a regular basis, please seek direction from the organisation's head office/management, seek advice from the Office of the Irish Data Protection Commission (www.dataprotection.ie), or contact Sytorus at info@sytorus.com for further information.

SCENARIO: CORRESPONDENCE WITH PARENTS, CLIENTS, STUDENTS OR STAFF

Division of Responsibility

Senior staff of the school/organisation should be responsible for the management of any communication which is sent out on official organisation note-paper or claiming to be on behalf of the organisation. This does not mean that only one person should send every communication. However, anyone sending communications or correspondence on behalf of the organisation or using the persons' (or parents') contact details to do so should be made aware that the communication, as well as the use of such personal data, must be in compliance with the GDPR.

The Irish Electronic Communications Regulations (2011) introduced specific obligations for any organisation using electronic media (calls to landline, fax or mobile phone, as well as SMS, e-mail or social media messaging, e.g., Facebook) to send marketing, promotional or fund-raising messages.

Servicing v Marketing Messages

The school/organisation can differentiate between 'servicing' or administrative communications which are integral to the day-to-day administration of the organisation, and which are expected by the parents/guardians and students due to the nature of the activities (such as reminders about events, exam and registration deadlines, notification of a change of time for parent/teacher meetings, or an up-coming in-service day, etc.) and 'marketing' or promotional communications, which the organisation sends in order to promote or advertise products or tickets to an event.

As long as the organisation's management sets reasonable expectations at registration, the sending of such servicing communications is permissible without prior consent.

However, under the 2011 Electronic Communications Regulations and the GDPR, the organisation must have **prior, clear, freely-given consent** from its staff and/or parents/guardians before sending out electronic marketing communications as described above.

Things to Do:

- For postal communication, the organisation should have headed note-paper, and only authorised members of staff should have access to such material, in order to control the number of people representing or speaking on behalf of the organisation.
- Anyone sending communications on behalf of the organisation should ensure that this is carried out with the prior awareness and approval of the school Principal/organisation's management.
- Anyone sending electronic direct marketing or promotional communications on behalf of the organisation, whether by e-mail, SMS or via social media, should ensure that they have the prior consent of the intended recipient to contact them in this manner. Consent here must be "freely given, specific, informed and unambiguous, involving an active indication of the individual's preference."
- Any direct marketing or promotional message must provide the recipient with the option or mechanism to "opt out", i.e., to decline to receive such messages in the future.
- Communications which are delivered by hand (e.g. sent home with young persons for their parents'/guardians' attention) or which are not addressed to an individual ("The Householder", etc.) do not need to comply with this obligation.

- Any communication from the organisation should include contact details for the sender or another staff member, in case the recipient needs to seek clarification or follow up on the content of the communication.
- The school/organisation should confirm the appropriate contact details for each member at registration – this includes the details of the parent(s) or guardian(s) to be contacted in relation to each underage or child member (those under 18 years of age).
- Where servicing messages are being sent via social media, WhatsApp or other group text facilities, it is important to ensure that the purpose and content of the message is confined to the purpose or purposes for which the messaging group was set up – for example, if the WhatsApp group was set up to inform parents about upcoming events, times of meetings or deadlines for registration, then the content of any message sent via this Group must be limited to those purposes. (Principle 2 – Specified and Lawful Purpose).
- E-mails sent by organisation officials to several recipients at once should always avail of the. bcc (“blind copy”) facility in order to prevent the unnecessary disclosure of recipients’ e-mail addresses to others (Principle 3 – Minimisation of processing).
- Where the school/organisation is made aware that the parents/guardians of a student may no longer be living together, the organisation should strive to ensure that both parents/guardians receive communication in relation to their child (unless otherwise agreed with both). (Principle 4 – keeping the personal data accurate and up-to-date).
- Servicing messages relating to the activities of children and under-age students (those under the age of 18) should be sent directly to their parents or guardians, not to the minors themselves.

Things to Avoid:

- The school/organisation/private practitioner should not correspond directly with any persons under 18 years of age. Any correspondence to juvenile members must be through their parents or guardians, using the contact details provided at registration. The organisation should take

reasonable steps towards confirming the authenticity of the parental consent, where appropriate.

- Where an organisation is aware that the clients'/student's parents may no longer be living together, they should avoid sending all communications to one or other of the parents, to the exclusion of the other.
- The organisation should not contact individuals for marketing or promotional purposes who have already asked not to be contacted for these purposes.
- The organisation should avoid sending promotional, fund-raising or marketing messages to individuals under 18 years of age.
- Since consent should involve an active indication of one's preference, the organisation should avoid using 'pre-ticked' boxes on any registration or application forms.
- The organisation should avoid making assumptions as to the consent or preferences of its staff, parents, clients and students. In particular, staff members should be consulted prior to being included in any promotional or fund-raising activities. Consent must be unambiguous, in order to be considered adequate under EU Law.

SCENARIO: REGISTRATION FORMS FOR ACTIVITIES

This section applies to registration forms for an organisation's activities, 'away days' and trips, as well as application forms for exams or client involvement in competitions or educational programmes.

Division of Responsibility:

The School Principal and Secretary should have overall responsibility for the management and processing of registration within schools. Year Heads and individual members of staff may collect the data directly from current and new students and their parents, but overall responsibility for the process rests with

the institution as the legal entity and Data Controller. In other organisations, the responsibility lies with senior management or with the practitioner in the case of those working in private practice.

In each case management should ensure that registration and application forms are designed to get the full range of data required from clients/students and parents (if the person is under 18) in order to meet the administrative objectives of the organisation, while being limited to seeking only the minimum amount of personal data necessary to satisfy these requirements.

Things to do:

- Ensure that the registration, application and competition entry forms include fields for all data items which are necessary to achieve the objective.
- Include contact details of the organisation's Data Protection Officer, where applicable, so that registrants or applicants can contact the organisation to seek clarification on any point.
- Ideally, organisations should have a nominated person responsible for the gathering and management of applicant data, who will be available to members (and their parents or guardians) to answer any questions they might have regarding the processing of such data.
- The organisation should familiarise themselves with the guidance around the designation of a Data Protection Officer (Article 37 GDPR). Public bodies and public authorities have an obligation to appoint a DPO, and even where the mandatory obligation might not apply, many organisations have seen the value in appointing a member of staff to be responsible for DP compliance.
- It should be noted that the GDPR permits several organisations to band together and have a single DPO – in this way, several schools/establishments in an area or town might decide to collaborate on the nomination of a DPO.
- At registration, all clients/students and parents must be informed about the purpose or purposes for which their personal data will be used. In

addition to the administration of their participation in the life/services of the organisation, this might include processing of subscriptions or bank payments and the sending of 'servicing' messages (e.g. notifications about events, dates on which the organisation is closed due to weather, elections or in-service training, etc.)

- If space permits, the form should provide a brief narrative for each field on the registration form, explaining why the data is needed and setting reasonable expectations with those providing their personal data regarding how that data will be used, and, where relevant, with whom it will be shared.
- Separately from registration purposes, in the case of those under 18 years of age, the registration form must offer parents a separate, clear option to 'opt in' to receive information about the organisation's promotional and fund-raising activities and events. This cannot be in the form of a pre-ticked box which individuals accept, but must be actively ticked by the person giving consent (both online and on paper forms)
- Where parents of a minor do not give their consent, the organisation should make sure that they are not contacted for these purposes. Parents must be offered an option of selecting an "*active opt in*" in order for this consent to be valid.
- The organisation should ensure that all completed registration forms are collated and brought to a central storage point as soon as possible, once the forms have been completed and submitted.
- Where possible, the organisation should minimise the amount of paper forms being used – where individuals (or parents/guardians on behalf a minor) register using paper forms, the organisation should try to transfer this information to computer as soon as possible, as data in this format is more secure and more efficient to store, manage, process and retrieve.
- Where it has been possible to type the details from paper registration forms into the organisation's computer system, the original paper forms should either be filed and stored securely in a central location or should ideally be shredded and destroyed. Schools should implement their own policy to this effect, encouraging good practice in the long term.

Things to Avoid:

- The form must not ask for individuals (or parents acting on their behalf) to provide data which the organisation does not intend to use – if there is no current processing requirement for it, the organisation should not seek the data on the registration form.
- The form should not label individual fields on the form as ‘mandatory’ unless there is a formal, legal requirement for that item of data. Where such a formal requirement exists, the organisation should explain the legal obligation associated with the item of data.
- The organisation should not assume that parents or staff will want to be contacted for marketing or promotional purposes, just because they are involved with the organisation or because their children attend. The form must offer individuals a separate option to actively opt in, NOT an option to opt out.

SCENARIO: MANAGING DATA SECURITY

Failure to keep personal data safe and secure is one of the biggest causes of breaches of the Data Protection legislation, and one of the most damaging things that can happen to any organisation, since it undermines peoples’ trust in the organisation, as well as damaging the organisation’s reputation and the credibility of its staff and their data management procedures.

Division of Responsibility

A senior member of school staff should be accountable for the data held by the organisation, controlling who has access to it, where it is stored, and how it is transported or transferred elsewhere. In addition, the organisation should adopt

a formal Data Protection Policy, outlining the safeguards and structures in place to maintain the security of the personal data under its control.

The responsibility for the security and safety of the personal data which is held by the organisation rests with each member of staff who has access to that data. Whether in paper or electronic form, the personal data is a valuable asset, and should be treated with the same respect as the organisation's premises and its fixtures and fittings.

The adoption of appropriate security solutions will vary depending on the volume, value and format of the data held by the organisation, and may include measures like encryption of laptops, mobile phones and storage devices (USB sticks, external hard drives, etc.), password protection on all files containing sensitive personal data, and locked cabinets at the organisation's offices in which all paper records are stored when not in use.

In particular, the organisation should consider differentiating between various categories of personal data, providing more stringent security measures for information which relates to the medical or psychological condition of clients/students and staff. In this context, interview notes and records of guidance counselling sessions should be afforded the highest level of protection.

The obligation regarding data security also extends to the physical security of the organisation's premises, the number of key-holders who have access to the premises and its individual offices, deployment of CCTV cameras on the organisation's grounds, etc.

Things to Do

- The organisation should have a Data Security policy which outlines the rules regarding acceptable use of the organisation's data, how it should be stored and transported, and who should have access to it.
- Any staff member who has access to the data should receive training regarding their responsibilities, should be familiar with this Security Policy and should adopt the appropriate security measures when processing the data.
- Whenever possible, the organisation should minimise the amount of personal data which is stored or processed away from the organisation's premises. Staff should be encouraged to minimise the amount of student or other personal data which they remove from the premises, and any material which is removed should be returned to the administration office as soon as possible.
- It is inevitable that staff members will hold their own records for classroom/client management and for teaching preparation (class lists, parent contact details, etc.), but such records should be kept to a minimum, and should be stored securely by the staff members while in transit or in use. This particularly includes circumstances where staff take data from the files or office in order to attend off-site meetings and conferences, etc.
- Where possible, the organisation should take a regular back-up of its electronic data records, so that in the event of a catastrophic incident (fire or flood damage to offices, etc.), normal activities can be restored in a timely manner.
- Senior management should challenge the 'need to know' of any staff members regarding the level of access which they have to client/student or parent data – access to data should be based on a person's specific role within the organisation, rather than simply because of the fact that they are on the staff.
- Where the organisation engages the data management services of any third-party, a formal Data Processor Agreement must be in place before any of the organisation's data is disclosed to the third party (a contract template is available from Sytorus, if required).

- The organisation's computer equipment should be password protected, and access codes should not be shared between staff, or left somewhere that is easily accessed.
- The organisation should adopt a 'clean desk' policy at its premises. Paper files should be locked away at the end of each working day, and when not in use.
- Data in both electronic and paper format should be transported and stored securely when being used away from the main premises and should be deleted or shredded once they are no longer required.
- Doors, filing cabinets and desk pedestals in the organisation's offices should be locked at the end of each working day, or when the offices are unoccupied.
- Staff should 'lock' their computer screens (by pressing CTRL + ALT + DEL) when they leave their desks unattended, even for a short time.
- The organisation should introduce a 'Leaver/Mover' policy to keep track of staff members, and the level of access they have to systems and data files. Where someone leaves the organisation, or moves to a new role, this should be logged, and their access to the systems should be withdrawn or changed appropriately, as soon as possible after their move or departure.
- Appropriate training, in the form of instruction at induction stage, regular refresher training, and this Guidance Handbook, should be made available to all staff of the organisation.
- Where CCTV has been deployed at the organisation's premises, the organisation should appoint a senior member of staff to be responsible for its maintenance and management. The Office of the Irish DP Commission provides separate, specific guidelines regarding the management and use of CCTV within an organisation, and the organisation should ensure that they are familiar with these guidelines.

Things to Avoid

- Data should not be stored on unencrypted or unsecured devices – Guidance counsellors and other staff who hold copies of personal data

on their personal computers or mobile device should ensure that those devices are password protected and secure.

- If possible, any electronic correspondence involving the personal data of staff, clients, students and/or parents should be conducted over secure, encrypted networks, rather than over publicly-available and non-secure networks such as Gmail or Hotmail.
- Where personal records are saved on a mobile device or laptop, they should be saved in a secure, password-protected folder, and never on the C:drive or desktop of the device.
- Paper records should not be removed from the organisation's offices unless it is absolutely necessary. Copies of personal data, used for a particular purpose or event, should be returned to the organisation's secured files as soon as possible and any unused or remaining copies should be destroyed as soon as that purpose or event is completed.

SCENARIO: BREACH MANAGEMENT AND NOTIFICATION

Division of Responsibility:

Under the GDPR, any incident which exposes staff, clients, parents' or students' personal data to risk must be notified to the Office of the Data Protection Commission within 72 hours of the organisation becoming aware of the breach.

The Commission has provided a form on its website (www.dataprotection.ie) which must be completed by the Data Protection Officer (DPO) or a nominated staff member, and which should include details around the incident, the circumstances leading up to it, its consequences, and what has been done to minimise the impact, as well as to prevent a recurrence.

Things to do:

- Once the organisation becomes aware of an incident or breach, the DPO or a senior staff member should be placed in charge of managing and investigating the incident
- All those involved in, or aware of the breach should be asked for their input regarding the incident, how it occurred, and the extent and impact of the breach (whether it involves the loss, destruction, disclosure or mismanagement of personal or sensitive personal data).
- The nominated incident manager should prepare a report on the incident, using the questions contained in the template provided by the DP Commission as a guide.
- Where the incident poses a risk to the data subjects whose personal data has been compromised (e.g. the loss of their contact details, bank details, the disclosure of sensitive or confidential information in relation to counselling, etc.) the organisation should send out a notification, either individually or through social or public media, to make them aware of this security breach, and the possible consequences, as soon as possible.
- Where a third-party organisation was involved in any aspect of the incident (e.g. an IT service provider or partner organisation), their input to the circumstances as well as the resolution of the incident should be sought as quickly and constructively as possible.
- The organisation should submit a report of the incident to the Office of the DP Commission as soon as possible once the details are known, but in any event, within 72 hours of first being made aware of the incident.
- The organisation should make every effort to retrieve or recover the data which has been compromised, as well as to put measures in place to prevent a recurrence. Where a system or process has been found to be insecure or faulty, the school should suspend their use of that system or process with immediate effect, until the cause of the problem can be identified and fixed.
- Once the cause of the breach is known, staff should be informed and provided with appropriate training to ensure that the risk of a recurrence is minimised.

- Where the breach incident is found to have been caused by unlawful or non-compliant actions of a third party, the organisation should invoke the appropriate clauses in the Data Processor Agreement to penalise the third party for any damage caused to the activities or reputation of the organisation, and any distress caused to the staff, clients, students or parents/guardians.
- Where the breach incident is found to have been caused by the mismanagement of personal data by a member of staff or a student within the organisation, the organisation should pursue appropriate disciplinary measures to penalise the individual involved, and to raise staff and client/ student awareness in order to prevent a recurrence.
- Any communication by the organisation in relation to the breach incident should be controlled and managed through the DPO or a senior staff member, to minimise misinformation and minimise the risk of worry or distress on the part of parents, clients or students.
- The organisation should initiate some form of training to raise awareness around the process for breach detection, evaluation and formal notification.

Things to Avoid:

- Where the breach incident poses a risk to the welfare or confidentiality of individual staff, clients, students or their families, the organisation should not consider suppressing or withholding information on a Breach from the Office of the DP Commission – to do so would be an offence under the GDPR. If the Commission were to become aware, at some point in the future, that the organisation withheld or failed to report the incident, the organisation could be prosecuted under Article 83 of the GDPR, with severe financial and reputational consequences.
- Where the organisation has confidence that the breach incident will not pose a risk to individual members or staff, there is no obligation to report to the Office of the DP Commission (e.g. where a laptop or USB stick is lost or stolen, but the device has been encrypted, there is no risk that the data contained on the device can be accessed, therefore no threat to the privacy of individuals).

- There should be no interim or unauthorised disclosure of information in relation to the breach incident – staff should refer any questions or concerns to the DPO or the senior staff member who has been nominated to manage the breach.
- The organisation should avoid any unnecessary delay in the notification process, both in respect of the Supervisory Authority and also the individual clients, students or parents whose personal data may have been compromised. Time is of the essence, both in terms of recognition of a breach and notification to the relevant authority or individual(s).
- Staff should receive training so that they are familiar with the detection and recognition of DP breaches that may occur inside the organisation, as well as being able to recognise the severity of the risk to the confidentiality and privacy of colleagues, clients, students and parents/guardians.

SCENARIO: REQUESTS FOR DISCLOSURE OF PERSONAL DATA

Division of Responsibility:

From time to time, the organisation may be asked to provide or disclose information about its staff, clients or students. In such circumstances, the organisation needs to exercise its responsibilities as a Data Controller of that data and set strong challenges to any such request for disclosure, until its staff can determine that the request for disclosure is legitimate, appropriate and lawful.

The management of the response to Subject Access Requests, which takes the form of a request from an individual staff member, client or student (or parent/guardian on their behalf if under 18) for a copy of their own personal data, is a specific provision within the GDPR, and will be treated separately later in this Handbook.

Things to do:

- The school Principal/organisation senior management or nominated staff member responsible for responding to such requests should challenge the basis for any request for disclosure of personal data held by the organisation.
- Even where a disclosure request is legitimate and justified, the organisation should only release the minimum amount of data necessary to satisfy the request.
- The organisation must be satisfied that the individual or organisation making the disclosure request is authorised to do so – whether they are a client, a student, the parent or guardian of a student, a member of An Garda Síochána, or an authorised officer of the Department of Education/Department of Justice/Department of Health or another, similar body.
- Registration forms used by the organisation should seek clear information on the identity of individuals (parents, guardians or family members) who are authorised to seek information on clients/students – this is particularly important where the parents of a young person may be living apart but are nonetheless equally involved in supporting the student's education and welfare.
- Staff of the organisation should be made aware of the specific legal and regulatory obligations which may apply to the disclosure of client/student data during the day-to-day operation of the organisation, for example due to Child Safeguarding.

Things to avoid:

- The personal data of staff, clients or students should not be generally available, and only the minimum amount of data should be provided or disclosed to those who request it, even where the request is legitimate.
- Unless permitted by law, information in relation to the guidance counselling or support being provided to a student should only be made available or disclosed with the clear, explicit consent of the client/student (to the extent that they have the capacity to give such consent).

- There is no automatic right of access, under Irish law, to a child's data by a parent or guardian – each request for disclosure of data must be validated on its own, separate merits.
- The organisation should never disclose staff, students' or parents' personal data, either individually or in volume, to another organisation without a legitimate justification for doing so. If requested, the organisation should act as the 'gate-keeper' for the data and should remain in control of any use of the data or any access to it.
- No personal data should be disclosed by an organisation unless a formal request in writing has been received, and unless the organisation has been able to verify the identity of the requestor, and their authority to request such information.

SCENARIO: APPROPRIATE NOTE-TAKING

Division of Responsibility

Staff members who provide guidance counselling services within an organisation must do so in compliance with the Codes of Practice set by the management authority of that organisation, as well as keeping in line with best practice in terms of client/student welfare, child safeguarding and note-taking. Guidance counsellors in private practice must work in compliance with the Code of Ethics of the Institute of Guidance Counsellors.

Any notes taken during the course of the provision of such services are highly confidential and must be treated at all times with the utmost care and attention. Ultimately, the organisation is responsible for their safety and secure storage, but the staff member responsible for taking and retaining such notes has a particular duty of care towards them, in order to protect the trust placed in them by the

client/student and parents, as well as to protect the quality and integrity of the guidance counselling process.

Things to Do:

- The identity of the client/student undertaking guidance counselling should be protected at all times. While it may be necessary to be able to identify the client/student from the notes taken, the guidance counsellor should take steps to mask or protect the client/student from being immediately identifiable;
- We recommend that the guidance counsellor uses initials or some form of code when referring to client/students during note-taking. The key to this code should be kept separately, and accessible only by the staff member providing the guidance counselling service, and, in exceptional circumstances, the School Principal/organisation senior management;
- Notes taken during guidance counselling meetings should be sparse, and should only include the minimum level of detail to enable the guidance counsellor to provide appropriate counselling, and to maintain continuity of care from one meeting to the next (Principle 3 – Minimisation of Processing);
- Notes taken in such circumstances should be retained and stored by the guidance counsellor directly, preferably in a lockable filing cabinet held separately from other client/student and organisation records;
- Any key which the guidance counsellor might employ in order to mask or protect the identity of the clients/students receiving guidance counselling should be held separately, and should only be made available to other parties at the discretion of the guidance counsellor, and with the best interests of the client/student in mind;
- The key to identifying client/students from guidance counselling notes should be held separately and should only be accessible by the guidance counsellor(s) and the Principal/organisation senior management;
- Notes taken should avoid any unnecessary reference to other demographic information – such as gender, parental circumstances, socio-economic circumstances or health information – which might inadvertently identify the individual client/student;

- The guidance counsellor should seek advice from appropriate authorities (Tusla, HSE, HIQA) regarding the appropriate retention of such notes, and the timely destruction of such material once its purpose has been fulfilled;
- Where the welfare of the client/student continues to be a source for concern, the guidance counsellor should continue to hold such notes on file, with a view to having a reliable record of the client's/student's welfare history if required as part of his or her continued care;
- The guidance counsellor should at all times adhere to practice guidelines for his or her profession in taking such notes, as well as in retaining, filing and storing them securely.

Things to Avoid:

- Where possible, notes should not make specific or unambiguous reference to the client/student in question;
- Notes taken during guidance counselling meetings should be held confidentially by the guidance counsellor, and should not be shared with or disclosed to others who are not actively involved in determining the best care for the welfare of that client/student;
- Even where other parties may become involved in the provision of care to the client/student, any disclosure of such notes must be done discretely, and only to the minimum level necessary to achieve the desired objective – that of providing optimal support to the client/student in question;
- The code (pseudonym) used to mask the identity of the clients/students receiving guidance counselling must be held separately and should not be generally available to other staff.
- Such codes should be of a different format to other codes or pseudonyms being used by other departments within the school or organisation, so that any inadvertent disclosure of other information would not also lead to the disclosure of the identity of the clients/students.
- Any case histories, multi-agency conferences or references made to the client/student receiving guidance counselling should avoid any direct reference to their identity, or to the specifics of their welfare, family

circumstances or status in order to protect the identity and confidentiality of the client/student and their family members at all times.

SCENARIO: MANAGEMENT OF CONSENT

Division of Responsibility:

Under the terms of the GDPR and the Irish Data Protection legislation, any organisation processing the personal data of living individuals must be able to reference a lawful processing condition in order to justify such processing.

These conditions include having the individual's consent, having a contractual obligation with the individual which necessitates such processing, having concern for the individual's welfare or health, or where such processing is in the legitimate interests of the organisation and is not at risk of intruding on the rights and freedoms of the individual. These justifications are found within Article 6 of the Regulation, and at least one such condition must apply in order for the processing to be lawful.

Where the data being processed belongs to the special categories of processing recognised in the legislation – including information on ethnic identity, religious conviction, ideological beliefs or the individual's mental or physical well-being – the organisation must be able to justify such processing with reference to a separate set of lawful conditions, derived from Article 9 of the Regulation. For the processing of such categories of data, at least one condition from Article 9 must apply in order for such processing to be lawful.



The GDPR considers that an individual aged 16 or older is in a position to provide consent, as long as they have the capacity to understand the circumstances of such a decision. For students under the age of 16, parental or guardian consent is required on behalf of the student, in order for the consent to be lawful.

However, both the GDPR and the Irish DP legislation recognise the value of clients/students aged under 16 being able to request and avail of guidance counselling services without requiring specific consent from parents or guardians.

Under both Article 6 and Article 9, the Consent of the individual, or of their parents or guardians, qualifies as an appropriate justification for the processing of such data. Section 9(c) of the Irish Education Act (1998) requires schools to make counselling services available to students. In most instances, the consent of parents or guardians is sought when doing so, but this is not always possible or necessary.

The GDPR has refined the understanding of consent by setting clear criteria which must be met in order for the consent to be considered lawful.

Under the GDPR, consent must be:

Freely given – there can be no conditions or ulterior motivations in providing consent;

Informed – the individual should be aware of the context and implications of giving consent;

Clear – it should be clear to the individual what they are consenting to;

Unambiguous – there should be no confusion or doubt as to the circumstances; and

An active indication – there should be no assumptions or conclusions derived from silence – the individual should be offered a means by which they can provide an active indication of their preference (no pre-ticked options or preferences on an application form, for example).

Where possible, the organisation should maintain a record of this active indication – for example, a signed registration or consent form, as evidence that the consent was lawfully and fairly acquired.

Things to do:

- When seeking consent, the organisation should recognise the dignity and identity of the client/student, while at the same time involving their parents or guardians, where it is appropriate and reasonable to do so;
- We recommend that any client/student seeking or availing of the guidance counselling services offered by the organisation should complete a registration form, on which the conditions and commitments of the organisation towards the client's/student's welfare and confidentiality are made clear;
- Where the client/student is unable to do so, or lacks the capacity to understand the consequences of such a decision, seeking the consent of their parents or guardians should be considered prior to the commencement of the guidance counselling service. However, we are mindful that this will not always be possible or in the individual student's best interests, and the school will need to evaluate each situation on its merits;
- At all times, the guidance counsellor should follow best practice for his or her profession in determining the wording and format of any such consent form and outline of associated conditions;
- Any form completed by the client/student, his or her parents or guardians should be retained by the organisation and held on file in relation to that client/student, observing appropriate measures to

protect the integrity and confidentiality of the client/student, their parents and family members;

- Consent should be revisited and renewed at the commencement of each year, in order to re-engage with the client/student and their family, and to ensure that they continue to be willing to participate in the guidance counselling service provided by the organisation;
- The school should remember that consent is not always necessary for such processing and that the welfare and interests of the student should always set the priority when processing personal data.



Things to avoid

- Organisations are advised to remind parents that guidance counselling is an integral part of school services and request that parents give consent for such services upon enrolment of the student. This can then be renewed on an annual basis.
- It should not be assumed that consent remains in place indefinitely – we recommend that consent, even where it has been actively and unambiguously acquired from the student or his or her parents or guardian, should be revisited and renewed at least on an annual basis;
- Where parental or client/student consent for certain processing was acquired prior to 25th May 2018, there is a risk that this consent will no longer satisfy the criteria set down by the GDPR (see above). Where this is the case, and where consent is being relied-upon for the data processing, the organisation should re-engage with the parents or client/student and re-confirm their consent for the particular processing, in terms which will clearly satisfy the GDPR criteria;
- Consent for one service should not be conflated or confused with consent for another – where the organisation proposed to extend or expand on the range of care or services being provided to the client/student, separate consent should be sought for each such service

- the consent for one service should not lead to an assumption that the client/student has given consent for another.

SCENARIO: RECORDS RETENTION AND DESTRUCTION

Division of Responsibility:

Organisations will need to keep certain categories of personal data for different periods of time – in some cases, in order to provide its registration and administrative services, in other cases to meet its legal or regulatory obligations or to maintain a historical archive of the organisation. The organisation needs to strike a balance between satisfying its legal and archival obligations and minimising the risk of data loss by removing or destroying any data which is no longer required for operational purposes.

The difficulty for many organisations is in deciding what personal records to keep and what to destroy. With electronic records, today's technology allows organisations to keep data for much longer, at very low cost. Paper records can eventually take up a lot of space and become a nuisance for the organisation if they are not properly managed and efficiently and securely stored.

The key principle of the GDPR is that the organisation is encouraged to keep the data only for as long as necessary in a format in which the individual is identifiable, in order to achieve its operational and legal objectives (e.g., administration of membership, processing of payroll and employment obligations, reporting to government departments and other national bodies, retaining information for insurance or legal purposes, etc.).

Therefore, it is not a question of the organisation's IT network or system capacity or the available storage space, but of how soon the personal data records can be destroyed or removed.

Things to Do:

- The organisations should be aware of its legal obligations in terms of retaining administrative, welfare and financial records – for reference, check the guidance on the website of the Office of the Irish DP Commission, at <http://www.dataprotection.ie>.
- The organisation should draft a Data Retention and Destruction Policy, including a Retention Schedule for the various categories of personal data being processed, based on these obligations;
- The organisation's Management, Principal and/or staff who have access to personal records should be aware of these Retention and Destruction Policies, and they should ensure that records are only kept for as long as necessary with reference to such Policies and Schedules;
- The organisation needs to remember that the retention obligations apply equally to electronic and paper-based records;
- As much as possible, personal records of staff, clients, students and parents which might be processed remotely or removed from the premises from time to time should be collated and returned to the organisation's premises in a timely manner for longer-term storage and retention;
- Once it has fulfilled its operational objectives and is no longer required by the organisation, any correspondence which contains personal contact details, whether old letters and invoices, application and registration forms, etc., should be shredded before being disposed of in an environmentally friendly manner,
- The organisation's master records should be held at the organisation's premises, and in secure storage, rather than spread among several the organisation's staff and departments. The exception to this recommendation would be the welfare guidance and guidance counselling notes and consent forms relating to such services;

- Computer equipment used by the organisation to process personal data should be wiped or de-gaussed with an industrial magnet to remove any trace of the data prior to the device being sold, decommissioned or recycled;
- Where an organisation relies on the storage, retrieval or shredding services of a third-party organisation in the management of its records and archives, the organisation must insist on having a Data Processor Agreement in place prior to the provision of such services (see the scenario in relation to Third Party Service Providers below).

Things to Avoid:

- An organisation should not keep records for longer than agreed in the Retention Schedule;
- The organisation's Board of Management, Principal and/or individual staff members should not keep copies of the organisation's personal data records at their homes when the original records have been destroyed as part of the Retention and Destruction Policy;
- It should be remembered that the school/organisation is the Data Controller, carrying ultimate responsibility for the acquisition, storage, security and retention of the data. No individual member of staff, whether directly employed or under contract, should take it upon themselves to shred, remove or anonymise personal data records without the knowledge and approval of management;
- Personal data in paper form should not be simply thrown in the rubbish – records containing personal data or special categories of information should be securely shredded before being disposed-of;
- Computer equipment on which the organisation's data had been processed should not simply be sold on or recycled without first being professionally 'wiped' to delete any personal data from the hard drive.

SCENARIO: INVOLVEMENT OF THIRD-PARTY SERVICE PROVIDERS

From time to time, the organisation may need to engage the services of a third-party specialist to assist them in their work – for example, a recruitment company to find new staff, an accounting firm to help with completion of the organisation’s accounts, a guidance counsellor to support students or an IT service provider to install and maintain the organisation’s hardware and applications network infrastructure.

Where these third parties will have access to the personal data held by the organisation, (whether or not this is directly intended) they are known as Data Processors, and the organisation must ensure that a formal contract, known as the Data Processor Contract, is in place before the third party service provider gains access to any of the personal data held by the organisation, in either electronic or paper format.

Division of Responsibility:

While the third-party service provider may produce their own contract template for this purpose, the obligation to ensure that such a contract is in place rests with the Data Controller (i.e. organisation’s management)

Things to Do:

- The organisation must ensure that the third-party service provider being sought to deliver the service is competent, reliable and understands its obligations under the Irish DP legislation;
- The organisation must ensure that the formal, written contract is in place prior to the third-party service provider having any access to the personal data for which the organisation is responsible;
- The clauses of this contract must include reference to the various topics mandated for inclusion by the GDPR – including an obligation to confidentiality when processing the data, the security of the information

in question, an obligation to process the data within conditions or parameters set by the Data Controller, etc;

- The terms of the contract should be reviewed on a frequent basis, at least annually, and the Controller must ensure that the Data Processor always complies with all terms of the contract while the data is being processed;
- Where the Data Processor engages the services of other organisations to further assist with the processing of the personal data (a sub-contractor), the Processor must notify the organisation in writing about this appointment, and the organisation must have the option to veto or challenge any such appointment.

Things to Avoid:

- Third parties must not be allowed unaccompanied access to the network, files or office premises of the Data Controller (e.g. the school) without this contract being in place – regardless of how short the term of engagement of the third-party service provider may be.
- At the end of the contractual engagement, the third-party service provider must not be allowed to keep the data disclosed to them during the course of the contract. The third-party must either return such data or provide the organisation with a written undertaking that any such data has been verifiably put beyond use or destroyed, unless there is a legal obligation or operational requirement to retain it for any purpose.
- The organisation should not simply engage a third-party service provider on a referral or recommendation – some effort must be made by the organisation to verify and evaluate the third-party provider's competence, qualifications and compliance prior to engagement.

SCENARIO: USE OF PHOTOS AND VIDEO IMAGES

Photographs and video images capture the personal data of individuals and must therefore be managed in compliance with the DP legislation.

Division of Responsibility:

As the organisation on whose behalf the images or footage is captured, the school/organisation is the Data Controller, and must therefore ensure that any processing of the images is done in an appropriate and compliant manner.

Things to Do:

- Where the organisation plans to capture photographs of an upcoming event or competition, those attending should be notified in advance, where possible. This might mean that the organisation places a notice on the poster or tickets to the event, such as 'Please be aware that photos taken at the event may be used by the school/organisation in the future for promotional and publicity purposes';
- At the event itself, we recommend that discrete but visible posters remind attendees that photographs and/or video footage will be captured.
- Where CCTV is in operation at the organisation's premises, clearly visible notices (the 'Fair Processing Notice') should be displayed, making staff, parents and clients/students aware that their video image is being captured, the purpose for doing so, and the contact details of the DPO or a senior staff member, should they have any questions or concerns;
- The CCTV system should be regularly serviced and maintained, so that the images captured can be used for the purpose for which the system was installed – namely, the prevention or investigation of unlawful or unauthorised activity, access to the organisation's premises, or misuse of the organisation's facilities;
- Where photos are taken at the event, the photographer should make it clear to those whose image is captured that the organisation would like to use the image, with their consent. Where their consent is forthcoming, the photographer should note the fact. Naturally, where anyone captured in the images objects, this photo should not be used by the organisation for any purpose.
- Where photographs taken at an event contain images of children or minors, the organisation must seek the clear consent of that child's

parents or guardians before using the image for any purpose in relation to the organisation;

- While it is not mandatory to get such consent in writing, we recommend that the photographer seeks to get clear, unambiguous permission from the individual at the time the image is captured, in order to avoid or prevent any dispute with regard to the use of the image in the future;
- Where the organisation engages the services of a professional photographer to capture images during an event or competition, the organisation must put a Data Processor Agreement (see above) in place with the photographer beforehand, setting clear expectations regarding their capture, use, storage and retention of such images.
- Photographs and images should be stored and indexed with reference to the event at which they were captured, and the individuals depicted in the images, in order to be able to retrieve the images at some point in the future if they are requested for disclosure or publication.

Things to Avoid:

- Photos and images taken at school/organisation events should not be published without the clear awareness of the individuals captured in those images. Where it is not possible to get permission from everyone in the image (for example, a large crowd or grouping), the organisation should make every effort to make them aware, beforehand, that images and/or video will be published on the organisation's web-site or posted on social media, and remind them that they have the option to object to such use of their image at any time;
- Photos, videos and images should only be held for as long as they are useful and relevant to the work and activities of the organisation and should then be either archived or destroyed;
- Photo, videos and images (including CCTV) should only be used for the purpose for which they were captured, and staff should not have open or unlimited access to such images, in order to prevent or minimise the risk of their unauthorised or excessive use.

SCENARIO: RIGHT OF ACCESS REQUESTED BY THE DATA SUBJECT

In compliance with the GDPR, any individual whose personal data is held by the organisation has the right to receive a copy of the personal data that is being kept about them by the organisation, either on computer or held in manual (paper) format in a filing system.

Any person who wishes to invoke this right can submit a valid Subject Access Request (SAR). There is no formal template for such a request. A request is valid once it meets the following two criteria:

- The request must be writing;
- The requestor must provide adequate proof of their identity.

Things to do

- The organisation should seek to verify the identity of the requestor as soon as possible once the access request has been received. No search or collation of data should commence prior to the verification of the individual's identity;
- The organisation will have a maximum period of one month to respond to a valid request. The organisation should try to respond to the request in the shortest possible time.
- A staff member should be nominated to co-ordinate a reasonable search for the personal data which relates to the requestor.
- As soon as possible, the nominated staff member should begin collating any records which make a clear reference to the requestor;
- Where a third-party service provided supports the organisation in storing, archiving or holding data records, the nominated staff member should liaise with these third parties in order to conduct an equivalent search for references to the requestor among any material held by them;

- Any collated documents which also make reference to another person should be modified or redacted so that only the reference to the requestor remains legible;
- Once a reasonable search for material has concluded, a copy of the resulting data should be dispatched to the requestor in printed format using registered post, so that a verifiable record of receipt can be acquired as proof of delivery;
- The organisation should also keep a full copy of the data provided, in case there is any subsequent dispute over the contents or scope of the data provided.
- There are some exemptions to this obligation under the GDPR, including circumstances where the organisation cannot location any reference to the individual, or where management might reasonably feel that disclosure of certain data might cause distress to the individual requesting the data, or to their family.

Things to avoid

- The organisation cannot charge a fee for responding to this initial access request. However, a reasonable fee can be charged subsequently, where the individual requests a copy of the material already provided.
- Original documents should never be disclosed as part of a response to a Subject Access Request.
- While the organisation should conduct a reasonable search of its systems and records for any reference to the requestor, there is no obligation to search through back-up material, since this is just a copy of data already contained in the 'live' system.
- The organisation should not disclose personal information which, in the view of qualified individuals, might cause distress to requestor. This may apply in the case of notes and observations made by a doctor or guidance counsellor, for example.

RESPONDING TO DATA SUBJECT RIGHTS

While this Handbook focuses on the obligations and activities of guidance counsellors, we should remember that we are *all* Data Subjects, by virtue of the fact that the organisation is processing our data as staff, parents, clients, students, etc. The Data Protection legislation provides specific rights for Data Subjects, in addition to the set of Principles mentioned earlier in this Handbook. The following Rights are available to anyone whose personal data is being processed by a school/organisation:

- The right to access a copy of their data held by the organisation, as outlined above
- The right to have incorrect data, which relates to them, either corrected or removed
- The right to 'opt out' from receiving direct marketing material
- The right to prevent processing of their personal data which would be likely to cause damage or distress
- The right to have processing explained where decisions are made solely by automated processing
- The right to support from the Office of the Data Protection Commission
- The right to seek compensation in the civil courts, in the event that we feel our personal data has been misused causing us distress or reputational damage
- The right to be Forgotten/ Erasure – the right to have our personal data removed from use, unless the school has a lawful reason for retaining it
- Right to Data Portability – the right of an individual to request that their personal data be 'ported' or moved from one organisation to another – e.g. to another school, a bank, insurance provider or utility.

Under GDPR legislation, when any of these Rights are invoked by an individual, the school/organisation must be able to respond in a timely and appropriate manner, within no more than one month of receipt of the written request. An organisation cannot charge a fee for its response to these Rights.

COMPLIANCE WITH OTHER STANDARDS AND REGULATIONS

In addition to the GDPR / Irish Data Protection Act, all organisations must comply with obligations under a wide range of other legislation and standards, including education, employment and tax law, anti-money laundering, credit card security (PCI DSS), health and safety, child safeguarding, etc. In some cases, compliance with one obligation may appear to contradict or compromise compliance with another.

For example, in responding to a request from the Gardai for disclosure of details about a student, that person's privacy rights and confidentiality may have to be set aside due to the over-riding concerns of the Gardai with regard to their investigations.

Where such a conflict arises, the organisation should feel free to seek legal advice, or to seek advice from the Office of the Data Protection Commission, before disclosing the data.

FURTHER INFORMATION AND REFERENCES

Further, detailed information on Data Protection is available from a number of sources:

The office of the Irish Data Protection Commission at www.dataprotection.ie

The Office of the DP Commission has provided specific Guidance for the Irish Charity and Voluntary Sector at <http://www.dataprotection.ie/docimages/CharityMarch14%201.pdf>

APPENDIX I - FREQUENTLY ASKED QUESTIONS

Q. Are the GDPR obligations different for students under and over 16 years of age?

A. No – the GDPR, as well as the Irish legislation, makes clear that no additional consent or parental approval is required by a student under or over the age of 16 when availing of counselling or support services – for that reason, the same form will work equally well for both age demographics.

Q. How can we redact the names of all students mentioned in our notes and still follow the thread of who did what, e.g. bullying cases which can involve groups of students?

A. This will be discretionary on the part of the guidance counsellor – the notes must be clear enough to achieve the appropriate objective, the provision of professional counselling, while protecting the privacy and confidentiality of all concerned. This is not stipulated in the GDPR legislation, nor are guidelines available within the legislation.

Q. Do we need permission from parents to keep records?

Not necessarily, given that the guidance counsellor's reason for retaining some records may be based on their statutory or contractual obligations under employment, as well as for Child Welfare or Safeguarding purposes. However, we recommend that parents are made aware of the fact that their children's' data is being held and processed by the organisation, as well as the reasons for such retention and any information in that regard which is relevant in the interests of transparency and openness – e.g., if the data is being (or is likely to be) processed by a third party, or is being held for a disproportionate period of time – e.g. long after a child may have finished at a particular school.

Q. I have been recently told that I should not ask for permission for students to see me for guidance counselling - I had done this for years as we were informed in training that it was good practice. I was advised that this should be

mentioned by the Principal as one of the school services and that accepting a place in school implied acceptance by the school that I could see students - should this then be mentioned in the Admissions Policy or, if not, where?

A. This is not strictly a DP issue, but most likely covered by DES or Tusla guidance and best practice. If it is any help, the GDPR stipulation that a child aged 16 or under requires parental or guardian permission in order to set up a social media account does not apply where that child is seeking guidance counselling or support services.

An extension of that logic would imply that a child can avail of or approach a guidance counsellor without recourse to parental or guardian permission, and inversely, that a guidance counsellor can engage with a student without needing separate permission to do so.

Best practice indicates that parental/guardian consent should be sought, other than in cases where such consent is not possible, or would compromise the welfare of the student (for example, in cases where a parent is not motivated by the best interests of the student, and might deliberately seek to 'block' the student's access to such services).

Q. We were told recently that there was no issue with us keeping names on meeting minutes as long as they were secure, as, with time, people forget initials and who they relate to. Is this ok under GDPR?

A. The GDPR has no specific guidance on note-taking – the key related Principles would be Principle 3 – Minimisation – that only the minimum of personal data is captured and processed in order to achieve the objective, and Principle 6 – Security – that the data is at all times held securely, with the level of security determined by the value, volume and sensitivity of the information concerned.

Given the relative confidentiality of such guidance counselling notes, we would always recommend that any identifying elements are kept to the minimum, or codified, with the key to the coding held separately

Q. Under the GDPR, will I will now have to take the students' names off my guidance counselling notes and set up a system whereby anyone breaking into the locked filing cabinet could not identify the students from my notes? How

does this work in terms of Bullying incidents where you could have 4/5 people involved? Can initials no longer even be used?

A. Ultimately, the guidance counsellor must decide – as outlined above, as long as the storage and retention of these notes is sufficiently secure and limited, there should be no problem with individuals being identifiable directly from the notes. If, however, the files are stored in a cabinet with other documents, or to which other staff have access, then some level of codification/anonymisation/masking of the identity of the individuals is certainly preferable.

In the end, the volume and sensitivity of the personal data will determine the extent to which its security will need to be protected.

Q. At my school, we have had robust discussions over the last two years about whether or not I should be putting dates of Guidance Appointments up on VS Ware or not. The VS Ware notes in our school are available to be seen by Management and Year Heads and me. This would be under the individual student's records. This is not available to subject teachers. Is this correct from an IGC and GDPR perspective?

A. Again, there is no specific guidance within the GDPR, but this may be considered to be excessive – other staff have no need to know the details of the student with whom the guidance counsellor is meeting, and such identifiable information should be held securely and confidentially, not published in a forum to which others have access.

The fact that a student is seeking or undergoing guidance counselling could, in itself, qualify as Sensitive Personal Data, deserving an additional level of protection under the Regulation.

If, during the provision of guidance counselling, other parties need to be informed or included, then that decision will be at the discretion of the guidance counsellor, but we would recommend that it is not generally available, even to a small group within the school.

Q. I am a self-employed guidance counsellor – how does the GDPR apply to me?

A. As a self-employed practitioner, the guidance counsellor is a Data Controller, and primarily responsible for the personal and sensitive personal data which they acquire, store and process. All seven of the GDPR Principles outlined in this Handbook apply directly to the self-employed guidance counsellor.

Where the self-employed guidance counsellor works with a school under contract, then the School is the Controller, and the guidance counsellor is a Data Processor. A formal, written contract must be in place to govern the parameters of this arrangement, ensuring that any personal data gathered and held by the guidance counsellor during this contract engagement is managed in a compliant and appropriate manner.

Appendix II - 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 information (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 complying with such obligations
- Contact details through which a Data Subject can register any data management concerns with the organisation



*Note – A Data Protection Policy template is available from Sytorus, if required. Please contact Sytorus at info@sytorus.com, or call us at (01) 683 3312.



Sytorus Data Protection Consultancy

We would like to thank Hugh Jones and Sytorus for their participation in the development of this Data Protection Handbook.

Sytorus is an independent Data Protection consultancy offering specialist services regarding all aspects of compliance with the Irish and EU DP legislation, including assessments, training and practical advice.

Their online portal, Privacy Engine, helps organisation and Data Protection Officers to consolidate and manage their GDPR material, and to comply with the specific obligations of the legislation.

Sytorus Ltd. is based at Suite 243, The Capel Building, St. Mary's Abbey, Dublin 7.

Telephone: (01) 683 3312 or (087) 241 6892.

E-mail: Info@Sytorus.com.

Web: www.sytorus.com or www.PrivacyEngine.io