TOWARDS HEALING

A Catholic Church response to Institutional/Clerical/Religious abuse

Data Protection Policy

(Data Protection Act's 2018)

July 2018

Contents

Towards Healing

Towards Healing is an independent organisation providing professional support for people who have experienced institutional, clerical or religious abuse in Ireland.

This policy replaces Towards Healing Data Protection and Confidentiality Policy dated March 2015 and bring the organisation in line with the General Data Protection Regulation (GDPR).

All officers and agents of CCSS T/a Towards Healing ('Towards Healing') are obliged to comply with the Data Protection and confidentiality provisions set out in the Employee Handbook.

The General Data Protection Regulation (GDPR) very significantly increases the obligations and responsibilities in how we collect, use and protect personal data. At the centre of the new law is the requirement to be fully transparent about how we are using and safeguarding personal data, and to be able to demonstrate accountability for the data processing activities.

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Towards Healing. This includes obligations in dealing with personal data, to ensure that the organisation complies with the requirements of the relevant Irish legislation ('the Data Protection Act (1988), the Data Protection (Amendment) Act (2003) and the European Union General Data Protection Regulation (May 2018)), as enacted in the Data Protection Acts', 2018. which came into effect on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

Towards Healing is a Data Controller and the Data Protection Officer (DPO) is in charge of the administration of this policy for the purposes of compliance with the requirements of the European Union General Data Protection Regulation (May 2018). The following pages sets out details of the Data Protection Commission, the Acts, The Definitions, the Principles and Towards Healing Policy requirements for such compliance when data is being collected and when data is being processed through, for example, reporting to relevant authorities.

The Board of Directors of Towards Healing at its Board meeting on February 14th, 2018 appointed a Data Protection Officer ('DPO'). Two assistants - Clinical Director and the Chief Executive Officer will assist in carrying out the Data Controller responsibilities, with the DPO, however, the DPO retaining ultimate responsibility for administration of this Policy.

NB: Any person in respect of whom Towards Healing holds data, has the right to access their notes under Data Protection, Case Managers and all staff therefore, must be aware of the sensitivity of any material copied to files in respect of such persons, notably in respect of clients and therapists.

Data Protection Officer
Towards Healing
July 2018

Ireland’s Data Protection Commission

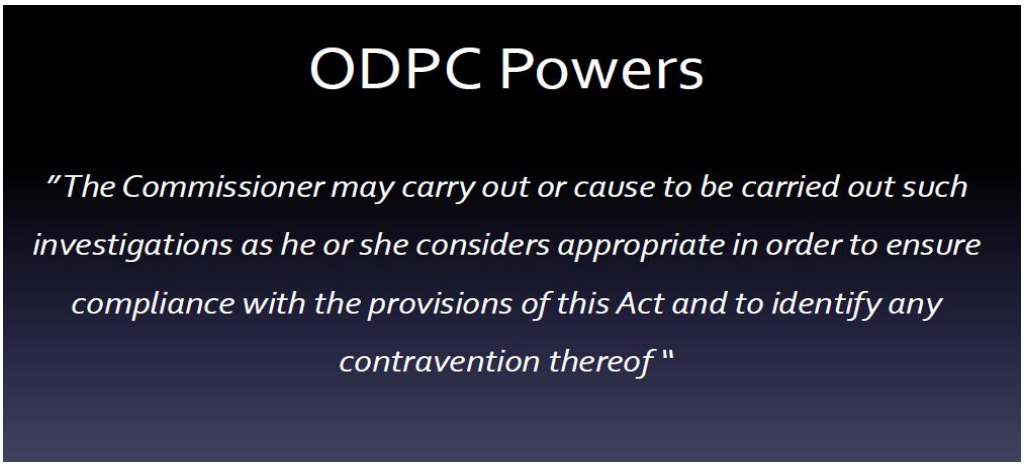
About the Commission

Data protection law is about your fundamental right to the protection of your personal data.

The Data Protection Commission was established by the Data Protection Acts 1988 to 2018 ('the Data Protection Acts').

Under the GDPR and the Data Protection Acts, the Commission is responsible for monitoring the application of the GDPR in order to protect the rights and freedoms of individuals in relation to processing.

The tasks of the Commission include promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, handling complaints lodged by data subjects and cooperating with (which includes sharing information with) other data protection authorities in other EU Member States.



Powers of the Commission

The Commission's Power to Enforce Compliance with the Act

Under section 10 of the Data Protection Acts 1988 and 2003, the Data Protection Commission may require a data controller or data processor to take whatever steps the Commission considers appropriate to comply with the terms of the Data Protection Acts Such steps could include correcting the data, blocking the data from use for

certain purposes, supplementing the data with a statement which the Commission approves, or erasing the data altogether. The Commission exercises this power by providing a written notice, called an "Enforcement Notice", to the Data Controller or Data Processor. A person who receives an Enforcement Notice has the right to appeal it to the Circuit Court.

It is an offence to fail or refuse to comply with an Enforcement Notice without reasonable excuse.

Investigations by the Data Protection Commission

Under Section 10 of the Data Protection Acts, 1988 and 2003, the Commission must investigate any complaints, which they receive from individuals who feel that personal information about them is not being treated in accordance with the Act, unless they are of the opinion that such complaints are "frivolous or vexatious".

With regard to complaints of breaches of the Data Protection Acts, the Commission is obliged to seek an amicable resolution of the complaint in the first instance. Where this cannot be achieved, the Commission may make a Decision on the complaint. The Commission's Decision can be appealed to the Circuit Court.

The Commission may also launch investigations on their own initiative, where they are of the opinion that there might be a breach of the Act, or where they consider it appropriate in order to ensure compliance with the Acts. In practice, the investigations to ensure compliance, usually, take the form of privacy audits. The Data Controller, normally, gets advance notice and the aim of the privacy audit is to assist in improving data protection practices. It is only in the event of serious breaches being discovered or failure of the Data Controller to implement recommendations that further sanctions would be considered.

The Commission's Power to Obtain Information

Under Section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commission may require any person to provide them with whatever information the Commission needs to carry out their functions, such as to pursue an investigation. The Commission exercises this power by providing a written notice, called an "information notice".

A person who receives an information notice has the right to appeal it to the Circuit Court.

Failure to comply with an Information Notice without reasonable excuse is an offence. Knowingly to provide false information, or information that is misleading in a material respect, in response to an Information Notice is an offence. No legal prohibition may stand in the way of compliance with an Information Notice. The only exceptions to compliance with an Information Notice are

(i) where the information in question is or was, in the opinion of the Minister for Justice, Equality and Law Reform, or in the opinion of the Minister for

Defence, kept for the purpose of safeguarding the security of the State, and

(ii) where the information is privileged from disclosure in proceedings in any court.

The Commission Power to Enforce Compliance with the Act

Under Section 10 of the Data Protection Acts, 1988 and 2003, the Data Protection Commission may require a Data Controller or Data Processor to take whatever steps the Commission considers appropriate to comply with the terms of the Data Protection Acts. Such steps could include correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commission approves, or erasing the data altogether. The Commission exercises this power by providing a written notice, called an "Enforcement Notice", to the Data Controller or Data Processor. A person who receives an Enforcement Notice has the right to appeal it to the Circuit Court.

It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

The Commission's Power to Prohibit Overseas Transfer of Personal Data

Under Section 11 of the Data Protection Acts, 1988 and 2003, the Data Protection Commission may prohibit the transfer of personal data from the State to a place outside the State. The Commission exercises this power by providing a written notice, called a "Prohibition Notice", to the Data Controller or Data Processor.

In considering whether to exercise this power, the Commission must have regard to the need to facilitate international transfers of information.

A Prohibition Notice may be absolute or may prohibit the transfer of personal data until the person concerned takes certain steps to protect the interests of the individuals affected. A person who receives a Prohibition Notice has the right to appeal it to the Circuit Court.

It is an offence to fail or refuse to comply with a prohibition specified in a prohibition notice without reasonable excuse.

The Powers of "Authorised Officers" to Enter and Examine Premises

Under Section 24 of the Data Protection Acts, 1988 and 2003 and under Regulation 19 of S.I. 336 of 2011, the Data Protection Commission may appoint an "Authorised Officer" to enter and examine the premises of a Data Controller or Data Processor, to enable the Commission to carry out their functions, such as to pursue an investigation. The authorised officer has the power to:

- enter the premises and inspect any data equipment there

- require the data controller, data processor or staff to assist in obtaining access to data, and to provide any related information
- inspect and copy any information
- require the data controller, data processor or staff to provide information about procedures on complying with the Act, sources of data, purposes for which personal data are kept, persons to whom data are disclosed, and data equipment on the premises.

It is an offence to obstruct or impede an authorised officer; to fail to comply with any of the requirements set out above; or knowingly to give false or misleading information to an authorised officer.

The Data Protection Acts

Irish Data Protection Act 1988:

- To regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically. (13th July 1988)

Irish / UK Data Protection (Amendment) Act 1988 / 2003

- The protection of individuals with regard to the processing of personal data and on the free movement of such data

EC (Privacy & Electronic Communications) Regulations, 2011

- Applying to the processing of personal data in connection with the provision of publicly available electronic communications services, including networks supporting data collection and identification devices.

EU GDPR

- The General Data Protection Regulation (GDPR) came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

Data Protection Acts' 2018 (Ire)

- Which enacts the EU GDPR

Key Definitions of GDPR

While the GDPR introduces several changes to key concepts in data protection terminology, many of the definitions from the 1995 EU Directive remain unchanged.

Data Subject
A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

Personal data
Personal Data is defined as ‘any information relating to an identified or identifiable natural person’. A Data Subject is ‘an identifiable natural person… who can be identified, directly or indirectly, in particular by reference to an identifier’.

Examples of personal data are not just a name or an identification number, but also online identifiers and location data. Crucially, personal data can also be ‘one or more factors’ combined together, which relate to the ‘physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data
A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one’s Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.

Processing Data
Processing continues to be defined as both automated and manual and is broadly interpreted. It can mean ‘any operation or set of operations which is performed on personal data or a set of personal data’. You do not need to view the actual data, but transmitting it, backing up a file or destroying data all count as a processing activity, even where the data is encrypted.

Data Controller
A Data Controller is a natural or legal person who ‘determines the purposes and means of processing of personal data’. (Towards Healing)

Data Processor
A Data Processor is a natural or legal person who processes personal data on behalf of the Controller but is not an employee of the Controller on the basis of a formal, written contract.

Under Irish law, both Controllers and Processors are considered to be the legal entities or organisations doing the work, not individuals.

Profiling
Profiling is ‘any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person’. Given examples relate to an individual’s likely behaviour, their reliability based on past performance, as well as their interests and personal preferences

Pseudonymisation
Pseudonymization is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. Pseudonymization, therefore, may significantly reduce the risks associated with data processing, while also maintaining the data’s utility. For this reason, the GDPR creates incentives for controllers to pseudonymize the data that they collect. Although pseudonymous data is not exempt from the Regulation altogether, the GDPR relaxes several requirements on controllers that use the technique.

Genetic Data
Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

Biometric Data
Biometric data are “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data".

Their processing for the purpose of "uniquely identifying a natural person” is prohibited.

However, it does contain some exceptions:

- If consent has been given explicitly
- If biometric information is necessary for carrying out obligations of the controller or the data subject in the field of employment, social security and social protection law
- If it's necessary to protect the vital interests of the individual and he/she is incapable of giving consent
- If it's vital for any legal claims
- If it's necessary for reasons of public interest in the area of public health.

Main Establishment

(a) A controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) A processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

Representative

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and

freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Supervisory Authority
Irish organisations report to the Office of the Data Protection Commission in Ireland, the 'Supervisory Authority', as defined by the GDPR.

Joint Controllers
GDPR introduces the concept of Joint Controllers, where two or more controllers jointly determine the purposes and means of processing. The organisations must set out a clear description of their respective responsibilities for compliance with the different GDPR obligations, in particular with regard to the rights of the data subject This might apply where organisations share data between them as peers, in a collaborative manner, rather than the more hierarchical relationship between a Data Controller and a Data Processor.

Data Protection Officer
A person appointed by the organisation to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients

Relevant Filing System
Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

The Seven Principles (Rebranded)

Article 5 which regulates the processing of personal data.

1. Fair & Transparent Processing (*Obtain and process information fairly*)

2. Specified and Lawful Purpose *(Keep it only for one or more specified, explicit and lawful purposes)*

3. Minimisation of Processing (*Ensure that it is adequate, relevant and not excessive)*

4. Accuracy and Current (*Keep it accurate, complete and up-to-date*)

5. Storage Limitation (Retain it for no longer than is necessary for the purpose or purposes)

6. Security and Confidentiality (*Keep it safe and secure*)

7. Accountability and Liability *(Use and disclose it only in ways compatible with these purposes)*

1. Fair and Transparent Processing:
Processing personal data needs to be based on one or several Lawful Processing Conditions. The Data Subject should have full and transparent knowledge of the identity of the parties to the processing, the purposes of the processing, the recipients of personal data, the existence of Data Subject rights and freedoms, and how to contact the Controller.

2. Specified and Lawful Purpose:
Personal data must be processed only on the basis of one or several specified purposes.

3. Minimisation of Processing:
Processing of personal data should be adequate, relevant and restricted to what is necessary in relation to the purposes for which they are processed. Not only will this relieve the organisation of the burden of performing actions on personal data, which are not required or necessary, but it will also reduce the overall risk of data breaches.

4. Accuracy and Current:
Personal data shall be accurate and where necessary kept up to date.

5. Storage Limitation:
Personal data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. Anonymisation or deletion is encouraged in order to minimise the length of time that personal data is held by the organisation. Some identifiable data may be kept for statistical, scientific or historical research purposes.

6. Security and Confidentiality:
Appropriate technical and organisational measures including encryption of data and computers is implemented to ensure a level of security appropriate to the volume and format of the data, its sensitivity, and the risks associated with it.

7. Accountability and Liability:
The Data Controller and the Data Processor will be required to demonstrate their compliance with the GDPR. The Data Controller is to continue to exercise reasonable care to ensure that the Data Processor carries out the processing in strict compliance with the GDPR.

Lawful Processing Conditions – Personal Data

Towards Healing Data Controllers will be required to be able to justify their processing of personal data, with reference to Lawful Processing Conditions, provided in the Regulation. Under Article 6 of the GDPR, the processing of personal data (e.g. name, address, mobile number, e-mail address, etc.) will be considered lawful only if at least one of the following conditions applies:

- ***Consent:***
  the Data Subject has clearly and willingly agreed to the processing of their personal data for one or several purposes.

- ***Contract:***
  the processing activity is necessary for the performance of a contract between the Controller and the Data Subject, or necessary at the request of the Data Subject prior to entering into a contract.

- ***Legal Obligation:***
  the processing is necessary for compliance with a legal obligation to which the Controller is subject - might be obliged to notify Tusla where the organisation become aware of allegations of child abuse).

- ***Vital Interests:***
  the processing of the personal data is necessary in order to protect the vital interests of the Data Subject.

- ***Public Interest / Official Authority:***
  the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller

- ***Legitimate Interest:***
  the processing is necessary for the purposes of the legitimate interests pursued by the Controller or the Processor, except where these are overridden by the interests or fundamental rights and freedoms of the Data Subject, particularly where he or she is a child.

Lawful Processing Conditions – Special Categories of Processing

Special categories of processing (processing of medical information, or information relating to race, religion, political beliefs, etc.), receive an additional level of protection under the GDPR. Such processing must be justifiable with reference to at least one condition from Article 9 of the Regulation – if this cannot be done, then the organisation should not be processing such information. When processing these special categories of personal data, the consent of the Data Subject needs to be explicit and cannot be implied or assumed.

The full list of Conditions from Article 9 is as follows:

- The Data Subject has given explicit consent to the processing of those personal data for one or more specified purposes; or

- The processing is necessary for the purposes of carrying out the obligations of the Controller or of the Data Subject in the field of employment and social security and social protection; or

- The processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent; or

- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim, in connection with its ethos and purposes; or

- The processing relates to personal data which are manifestly made public by the Data Subject; or

- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

- The processing is necessary for reasons of substantial public interest; or

- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to contract with a health professional; or

- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or

- The processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with the Regulation.

Consent Under the GDPR

The GDPR, introduces a new definition of consent for all purposes, not just Direct Marketing. Consent will now be any 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4.11).

In order to comply with this:

- Explain when and how you acquired the personal data of the Data Subject;
- Explain the purpose or purposes for which the data was acquired;
- Demonstrate the quality of the consent they have received

Where processing is based on consent, it is not necessary for the Data Subject to give his or her consent again if the original consent is in line with the conditions of the Regulation. In such circumstances, Towards Healing can simply continue to use the data as before.

However, where the original consent does not meet these criteria, it is necessary to conduct a data quality review.

Data Subject Rights and Freedoms

Besides the Seven Principles, the GDPR strengthens existing rights and freedoms of the Data Subject and introduces new rights and freedoms. The Data Subject is any living individual to whom the personal data relates.

The new rights and freedoms are:

- ***Right to be Forgotten***:

  this right to erasure of personal data allows the Data Subject to request from Towards Healing the deletion of personal data, without undue delay, on particular grounds. This right is important for Towards Healing where there may have collected personal data from a child in the past and where, as an adult, the Data Subject now has a different viewpoint of the risks involved in the processing. (Note that the general age of consent under the GDPR is 18 years and Ireland has introduced a national threshold of 18 years); This right is not absolute, and that in circumstances where the Controller can cite a legal obligation to retain the records, there is no obligation to erase or delete the data.

- ***Right to Restriction of Processing***:

  in certain circumstances, the Data Subject can request Towards Healing to restrict processing either permanently or temporarily. For example, the accuracy of data may be contested, there may be concerns that the processing may be unlawful or there are queries over the legitimate interests of Towards Healing overriding the rights and freedoms of the Data Subject.

- ***Right to Object to Certain Processing:***

  the Data Subject is entitled to object to the processing of their personal data based on his or her situation, preference or state of mind. Where data is processed, for example, for the purpose of direct marketing, consent may be withdrawn at any time and free of charge. An objection to processing may be overridden in certain circumstances. For example, Irish law may require the Controller to continue keeping fundraising records for financial auditing reasons. However, Towards Healing has to bear in mind that the burden of complying with such an overriding factor rests with Towards Healing, not the Data Subject.

- **Right to Data Portability:**

  where a Data Subject is moving their account from one provider to another, the Data Subject should be able to receive a copy of his or her personal data in a structured, commonly used, machine-readable format.

- ***Right of Access to Information:***

  where the Data Subject submits a written request, Towards Healing must provide a copy of any information relating to the Data Subject without undue delay and at the latest, within one month of receipt of the request. Any reference to other individuals in the data must be removed or redacted before the information is handed over. This deadline may be extended to two months in certain situations. There will be no fee for this facility under the GDPR

- ***Right to Complain, Right to Judicial Remedy***:

  where a Data Subject is not satisfied that Towards Healing adhered to its obligations under the GDPR, he or she can consider bringing a complaint to the Irish Data Protection Commission or seek a judicial remedy in the Irish courts.

Profiling and Automated Decisions

The GDPR, defines processing as an automated activity. Profiling is 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person'. Given examples relate to an individual's likely behaviour, their reliability based on past performance, as well as their interests and personal preferences.

Where an organisation uses an automated system or application in order to categorise personal data into groups of people who are likely to be interested in this campaign or that campaign, this is profiling as defined by the GDPR.

Using today's technological capabilities, organisations can determine, analyse and predict people's interests and habits to sophisticated standards and often without them realising fully the extent of the analysis that is being carried out.

This contravenes the Principle that processing needs to be done in a fair and transparent manner (Principle 1).

As a result, the Data Controller needs to assess and evaluate their profiling activities according to the Seven Principles. For example, they need to:

- ***Fair, lawful and transparent***: give full and easy-to-understand information on their processes and establish lawful processing conditions in relation to profiling.

- ***Specified and Lawful Purpose:*** define a specific purpose for the profiling, rather than leaving such activities open-ended or indiscriminate.

- ***Minimisation***: ensure that the minimum amount of personal data is acquired and used in the course of a profiling activity; restrict visibility to data in the course of profiling by applying pseudonymisation techniques

.

- ***Accurate and up-to-date:*** put regular checks in place to ensure the accuracy of the data used and that, as far as possible, all preferences of the Data Subject are up to date

.

- ***Retention and destruction***: define the retention period for which personal data is held in this context and where possible, anonymise data as soon as possible.

- ***Security & Confidentiality:*** implement adequate organisational and technical measures to keep the data safe both in terms of human error as well as IT systems. Train all staff appropriately.

- **Accountability** ***& Liability:*** where other parties are involved in the profiling activity, delineate liability and ensure full transparency.

GDPR requires further that where a Data Controller makes a decision based solely on automated processing, including profiling, the Data Subject will have the right not to be subject to such a decision. It is important here to note, though, that this only applies where the decision in question produces 'legal effects' or an effect which 'significantly affects' the individual concerned.

Organisations should heed the consent of the Data Subject as follows:

Profiling	Decision based on automated processing (this can include profiling) with legal or similar effect
Prior consent is not necessary, but Data Subject should be able to opt-out at any stage. Full information concerning the profiling activity needs to be provided to the Data Subject at first point of contact.	Prior consent is necessary - the GDPR says that the individual has 'a right not to be subject' to such decisions, so the default is that the Data Subject is offered a choice with regard to such activities.
Any objection will need to be accurately recorded in the database of the organisation and taken into account during any future profiling activity.	Where such a scenario does arise, prior consent needs to be recorded in the database, or an alternative decision-making process needs to be made available

Subject Access Requests

Any formal, written request by a Data Subject including an up to date copy of proof of Identity (passport, driving licence, public service card) for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed in line with the timeframe permitted by the Data Protection Commission (30 days)

Data Sharing and Overseas Transfers

Flows of personal data to and from Ireland are often obscure in the sector and could involve:

- Using services of third parties who are not in the European Union, such as a data analytics service or cloud hosting provider in the United States of America;
- Sharing personal data with friendly, like-minded organisation partners;
- Where an Irish organisation belongs to a global network of organisations, sharing data within that group;
- An international organisation processing personal data during the course of providing humanitarian services 'in the field'.

The increase of flows of personal data outside the European Union and the legislators of the GDPR hope to ensure that this does not undermine the rights and freedoms of the Data Subject. Transfers to third countries may only be carried out in full compliance with the GDPR. Transfers may occur:

- Where a country outside the European Union enjoys the status of 'adequacy'
- Where appropriate safeguards are in place, such as Binding Corporate Rules or Special Contractual Clauses in Model Contracts.

In the case of data transfers to and from the USA, the EU-US Privacy Shield is in place, which requires US companies to comply with certain principles and a defined enforcement regime. This Privacy Shield, together with the other international safeguards, are under constant review on an Irish and European level. DPOs and their respective organisations need to keep a watchful eye on developments in this area.

Where the Data Subject has given explicit consent, or the transfer is necessary for specific reasons as defined in the GDPR, the international protection mechanisms do not need to apply. It is therefore important for organisations to check which information about the intended processing was provided to the Data Subject at the point of first contact, and the clarity of consent which was obtained in relation to transfers of personal data overseas.

Supervisory Authorities

Irish organisations report to the Office of the Data Protection Commission in Ireland, the ‘Supervisory Authority’, as defined by the GDPR.

A noteworthy exception occurs where cross-border processing takes place and the decision concerning such cross-border processing are taken in another country. For example, one office of an organisation might be based in Dublin, but its international headquarters, responsible for its data management policy, might be based elsewhere within the EU.

Where such policy decisions are taken in another European country, the Supervisory Authority in that country becomes the ‘Lead Supervisory Authority’ and takes ownership of the matter, in cooperation with the Irish Commissioner.

Where the decisions are taken in a country which is outside the European Union, the legal entity who takes such a decision needs to appoint a ‘nominated representative’ inside the European Union, who will in turn report to the Supervisory Authority of the country in which it is processing personal data.

It is essential for Irish organisations to examine their operations to establish whether or not any cross-border processing takes place.

"Individuals must be able to enjoy the benefits of new technology, while at the same time remaining in control of their privacy"
Billy Hawkes, Data Protection Commissioner 2nd July 2011

Rationale

Towards Healing must comply with the Data Protection principles set out in the Data Protection Acts' 2018. This Policy applies to all Personal Data collected, processed and stored by Towards Healing in relation to its staff, service providers and clients in the course of its activities. Towards Healing makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by Towards Healing. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by Towards Healing and both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This Policy should be read in conjunction with the associated Subject Access Request procedure, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

As a Data Controller, Towards Healing ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage Towards Healing's data in a compliant manner will be viewed as a breach of contract and will be pursued through the Courts.

Failure of Towards Healing's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Towards Healing as a Data Controller

During its daily organisational activities, Towards Healing acquires, processes and stores personal data in relation to:

- Employees of Towards Healing
- Clients, Therapists and Suppliers of Towards Healing
- Funders of Towards Healing
- Members & Directors of Towards Healing
- Third party service providers engaged by Towards Healing

In accordance with the Data Protection Acts' 2018, this data must be acquired and managed fairly and legally. Not all staff members will be expected to be experts in Data Protection legislation. However, Towards Healing is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by Towards Healing, there is regular and active exchange of personal data between Towards Healing and its Data Subjects. In addition, Towards Healing exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with Towards Healing's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a Towards Healing staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the DPO to seek clarification.

The Data Protection Principles

The following key principles are enshrined in the EU GDPR legislation and are fundamental to Toward Healing's Data Protection Policy.

In its capacity as Data Controller, Towards Healing ensures that all data shall comply with all the Data Protection Rules. These provisions are binding on every Data Controller. Any failure to observe them would be a breach of the Act.

7 Principles - Policy

Towards Healing will meet their obligations in the following way.

(i) Lawful, Fair and Transparent Processing

For data to be obtained fairly, the data subject will, at the time the data being collected, be made aware of:

- The Legislation
- The identity of the Data Controller - Towards Healing
- Keeping of Notes - The purpose(s) for which the data is being collected
- Retention of Notes
- Data Sharing - The person(s) to whom the data may be disclosed by the Data Controller
- Right of Access
- Any other information that is necessary so that the processing may be fair.

The informed consent of the Data Subject will be sought before their data is processed;

- Where it is not possible to seek consent, Towards Healing will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;

- Where Towards Healing intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;

- Processing of the personal data will be carried out only as part of Towards Healing lawful activities, and Towards Healing will safeguard the rights and freedoms of the Data Subject;

- The Data Subject's data will not be disclosed to a third party other than to a party contracted to Towards Healing and operating on its behalf.

  If disclosure is required and following full discussion with the Data Subject, an Exchange of Information Form (EOI) will be sent to the Data Subject outlining why consent is required. When the EOI is received by Towards Healing, disclosure of Data Subject data will only then be disclosed to a third party.

(ii) ***Specific and Lawful Purpose***

Towards Healing will obtain data for purposes, which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which Towards Healing holds their data, and Towards Healing will be able to clearly state that purpose or purposes.

(iii) **Minimisation of Processing:**
Processing will be adequate, relevant and not excessive in relation to the purpose(s) for which the data is collected and processed.

Towards Healing will ensure that the data it processes in relation to Data Subjects is relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

(iv) **Accuracy & Up-to-date:**
Towards Healing:

- data will be kept accurate, complete and up-to-date where necessary.

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. Towards Healing conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.

- conduct regular assessments to establish the need to keep certain Personal Data.

- When a processor is speaking to a client regarding their service with Towards Healing, please ensure the note is entered on the client profile only.

- When a processor is speaking to a Therapist about Portal, Insurance, Contract TATP, CP (how to fill in), please enter note on therapist profile only.

- When a processor is speaking to a therapist about a client, please add the notes on client profile only.

- If a number of clients are mentioned throughout the conversation with a therapist, please add relevant notes to relevant client profiles.

(v) Storage Limitation:
Will be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.

Towards Healing will not keep data for longer than is necessary to satisfy the specified purpose(s).

(i) Client clinical records – 7 years after case closure

(ii) Therapist Records – Will only retain records on those who have provided services within past 7 years

(iii) For additional storage of records please see "document retention schedule".

Towards Healing has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format. "see document retention schedule".

Once the respective retention period has elapsed Towards Healing undertakes to destroy, erase or otherwise put this data beyond use.

Towards Healing will pseudonymise data for analysis purposes and will put a Do Not Contact (DNC) on the client and therapist profile.

(vi) **Security and Confidentiality:**

Towards Healing has employ high standards of security in order to protect the personal data under its care. Appropriate security measures have been taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Towards Healing in its capacity as Data Controller.

- Office 365 through Q Drive with appropriate authorisation to folders
- CRM System - Salesforce Platform

  Your data would be stored by Salesforce on secure servers within Europe and will be covered all relevant European data legislation. Salesforce has his is highly secure place for your data as Salesforce CRM is certified the safest in the planet place to store your information. For more information on the certification see https://trust.salesforce.com/en/compliance/ and https://trust.salesforce.com/en/
- Encryption of documentation on Data Subject profile
- Passwords updated regularly
- Password access to computers & CRM system
- Sage 50 Accounts
- Sage Quickpay
- Staff Contracts & Records
- ROS
- Bank of Ireland

Access to and management of all Data Subject records is limited to those staff members who have appropriate authorisation and password access.

(vii) Liability and Accountability

Any use of the data by Towards Healing will be compatible with the purposes for which the data was acquired.

Implications for Data Subject not providing consent

If no information is provided by the Data Subject, Towards Healing will not be able to provide any services.

Consent Under the GDPR

Where processing is based on consent, it is not necessary for the Data Subject to give his or her consent again if the original consent is in line with the conditions of the Regulation. In such circumstances, Towards Healing can simply continue to use the data as before.

However, where the original consent does not meet these criteria, it is necessary to conduct a data quality review.

Consent Data Quality Review

Towards Healing will carry out a Quality Consent Review of all records. This will be based on the 'Accuracy' Principle of the GDPR.

- **Accuracy**: Establish accurate records of personal details; and
- **Currency (up-to-date)**: Ensure that all contact details are up-to-date.

A quality review exercise will be carried out where there is uncertainty over the quality of consent given previously. Where certainty already exists, subjects will not need to be contacted in this way.

When carried out correctly, it will also allow the Towards Healing to:

- **Product and Service preferences**: Verify the individual's current status and preferences with regard to the organisation's products and services.

Towards Healing's intention to use the campaign solely to enhance the quality of the personal data already held, and to gain confidence regarding the quality and accuracy of that data.

Applying clean data management procedures will ensure that those Data Subjects who indicate their consent to be contacted for marketing purposes.

Those who exercise their right to 'opt out' and indicate they no longer wish to be contacted should be marked as "Do Not Contact" (DNC) for marketing purposes and should only be retained further by Towards Healing if there is an appropriate operational or contractual reason to do so.

Towards Healing maintains a single, consistent list of its clients/therapists/funders which is updated regularly and provides an accurate view.

Towards Healing must review its registration and clients/therapists/funders interaction details (registration forms, web-site query facility, etc.) to ensure that, from this point forward, any personal data acquired from Data Subjects offers the appropriate options to actively “opt in”, or to “opt out” and decline future marketing contact.

It is intended that by complying with these guidelines, Towards Healing will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party Processors

In the course of its role as Data Controller, Towards Healing engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation setting out as follows:

- 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 activities of the Processor.

In addition, the contract from Towards Healing provides clauses regarding the following responsibilities of the Processor, including:

- only processes the personal data based on documented instructions from Towards Healing;
- ensures that persons authorised by the Processor to process the personal data have committed themselves to protecting the confidentiality of that data;
- takes all appropriate measures required to ensure the security of the personal data
- respects the preferences of Towards Healing with regard to engaging another processor or sub-contractor;

- assists Towards Healing by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Towards Healing's obligation in responding to requests relating to a data subject's rights;

- assists Towards Healing in ensuring compliance with the obligations regarding data security, in as far as possible;

- that, at the choice of Towards Healing, the Processor deletes or returns all the personal data to the controller after the end of the provision of services outlined in the contract;

- makes available to Towards Healing all information necessary to demonstrate compliance with the obligations set out in the Regulation, and allows for and contribute appropriately to audits, including inspections, conducted by Towards Healing or another auditor mandated by Towards Healing.

Subject Access Requests

Any formal, written request by a Data Subject including an up to date copy of proof of Identity (passport, driving licence, public service card) for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed in line with the timeframe permitted by the Data Protection Commission (30 days)

As part of the day-to-day operation of the organisation, Towards Healing's staff engage in active and regular exchanges of information with Data Subjects.

The Data Subject will have the right of access to their personal data which was collected concerning him or her and can exercise that right easily and free of charge, in order to be aware of, and verify, the lawfulness of any processing which is being conducted. Towards Healing must respond within one month of receiving the valid, written request with up to date proof of identity.

Every Data Subject has the right to know, from Towards Healing:

- Who processed their personal data where, when and how;
- Why such data was processed;
- For how long such data was processed;
- The recipients of the personal data;
- Where applicable, the logic involved in automatic processing, including profiling and the consequences of such processing.

In addition, the requestor will be entitled to a copy of any personal information held by Towards Healing which relates to him or her.

The specific time-lines within which Towards Healing must respond to the Data Subject is 30 days from receipt of valid written request and up to date proof of identity,

Where the personal data might be held by a third party on behalf of the Towards Healing (e.g. by a Data Processor), Towards Healing needs to ensure that the Data Processor contract covers any circumstances where the third party will be obliged to assist in responding to a Subject Access Request.

As the Data Controller, Towards Healing must ensure that there is no delay in responding (within 1 month), even where some proportion of the personal data may need to be collected from a third party.

Procedural Obligations on Towards Healing

GDPR introduced procedural obligations on organisations who are involved in the processing of personal data Towards Healing and the Data Processor. Whilst some liability may be apportioned to the Data Processor or another Joint Controller, Towards Healing is the party which is principally responsible for the processing of the data in question.

Key responsibilities will include:

- ***Process logging:***
  Every processing activity needs to be recorded in a tracking system, which is maintained on an ongoing basis; adequate, documented reports on such processing activity needs to be available when requested by the Data Protection Commission the log must include such details as the parties involved, the purpose of the processing, the categories of personal data and Data Subjects, the recipients, any transfers outside the European Union, and so forth. The obligation to document a data processing log replaces the previous system of registering with the Data Protection Commission. The Processing log becomes a key mechanism to demonstrate compliance in the future. Process Logging only applies to organisations with more than 250 employees, in the case of Towards Healing this obligation applies due to the regular processing of sensitive data and/or conduct special categories of processing.

- ***Logging breaches:***
  Any personal data breaches of which Towards Healing or Processor are aware of must be documented, in line with the processing log system described above.

- ***Breach notification to the Office of the Data Protection Commission:***
  Towards Healing will notify the Data Protection Commission when all incidents which expose personal or sensitive personal data to risk. The deadline is 72 hours from becoming aware of such an incident. Any delay in reporting, beyond that point, must be explained with a reasonable justification.

- ***Breach notification to the Data Subject:***
  Where a breach is likely to result in a high risk to affected individuals, organisations must also inform those individuals without undue delay.

  Certain encryption or pseudonymisation techniques may prevent Towards Healing or Processor from having to notify the Data Subject, e.g. where a device containing personal data is lost or stolen, but the device itself is encrypted, the data is considered safe and no notification to the Data Subjects is necessary.

- ***Data Processing Contracts:***
  GDPR requires Towards Healing to enter into a Data Processing Agreement with each Data Processor who is involved in the processing of personal data on Towards Healing's behalf. This contract will be in writing and will cover certain basic requirements, such as guarantees concerning the safety and security of data, auditing rights, cooperation concerning the rights and freedoms of Data Subjects. A similar written agreement is in place where Towards Healing enters other arrangements, e.g. between two organisations in a group hierarchy; between Joint Controllers or where several Processors work together in one processing activity.

- ***Sub-contracting:***
  Towards Healing is to be made aware that where a Data Processor enlists another processor for carrying out specific processing activities on behalf of Towards Healing, it will be the responsibility for that Processor to ensure that the same level of protection exists for the data during this element of the processing, as exists between Towards Healing and the initial Processor.

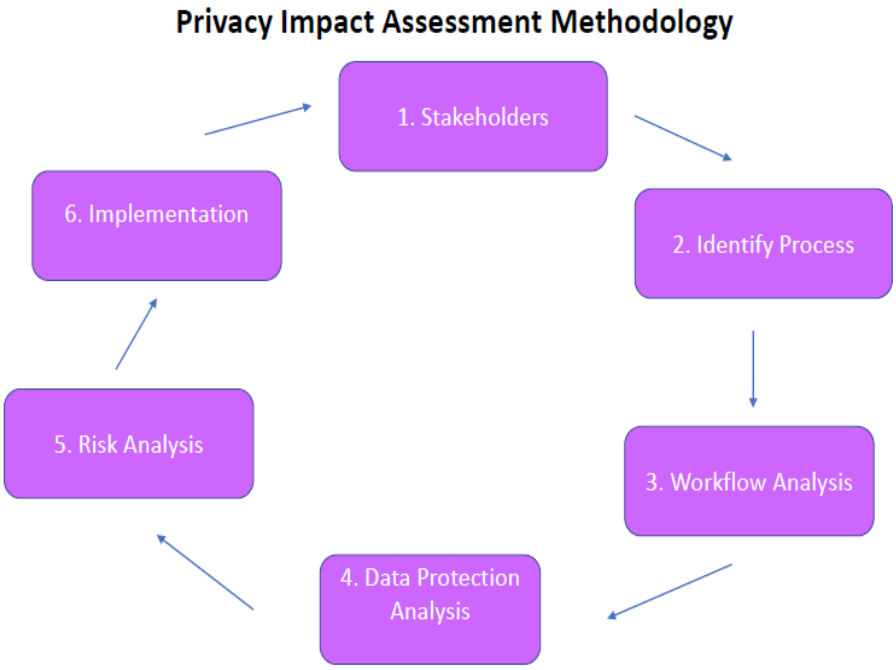
- ***Privacy Impact Assessments:***
  Where a significant change to data processing operations are likely to result in a high risk to the rights and freedoms of the Data Subject, Towards Healing is required to carry out a Privacy Impact Assessment (PIA) in order to evaluate the risks inherent in such changes. Attention will be given to the origin, the nature and the severity of the risk in question.

  The results of this Impact Assessment must be documented and retained and must be made available to the Office of the DP Commission (ODPC) on request. Any identified 'high risk' has to result in Towards Healing engaging with the ODPC before the processing activity in question begins.

- ***Data Protection by Design and Default:***
  In line with the requirement to carry out a Privacy Impact Assessment the principles of 'Data Protection by Design' and 'Data Protection by Default' place privacy and the rights and freedoms of the Data Subject at the heart of any current or future processing activity.

Towards Healing take the following conditions and measures into account when determining the suitability and practice of a Privacy Impact Assessment:

- Where the personal data processing is likely to give rise to a risk to the data;
- Should involve the DPO and other, relevant stakeholders;
- Systematic evaluation of proposed processing;
- Identification of risk;
- Outline of the measures being taken to mitigate those risks;
- Outline of structures and measures planned to achieve compliance;
- Where substantial risk is identified, the Data Controller must check with the Supervisory Authority.



Data Protection Officer

The Data Protection Officer ('DPO') plays a key role in ensuring that the Towards Healing and the Data Processor are compliant with the complex requirements of the GDPR. Under the Regulation, a DPO was appointed where one of the following criteria applied:

- where the organisation processes data in a manner which requires 'regular and systematic monitoring of Data Subjects on a large scale'

- where the data processing activities 'consist of processing on a large scale of special categories of data'; or

- where the organisation is a public body or has statutory authority, or processes personal data on behalf of such an organisation.

Towards Healing regularly processes special categories of personal data – data relating to an individual's physical and mental health and well-being, ethnicity, religious beliefs, criminal records, etc.

Key features of this role are:

- The DPO can be part-time, but no conflict of interest should impact his or her independence and impartiality when carrying out the role.
- The DPO may be an existing staff member or the role may be outsourced, but the candidate must demonstrate expert knowledge of the legislation, be sufficiently qualified and experienced, and understand the business model and data processing activities of the organisation in question;

- A direct reporting line to senior management should be established, so that the DPO can clearly report on data processing compliance, notify in the event of incidents and make suitable recommendations;

- The DPO must have sufficient resources available to him or her to do their job;

- The DPO cannot be penalised for his or her decisions, actions and recommendations in certain circumstances, and needs to be supported in an inclusive, collaborative manner.

The DPO will be required to:

- Inform and advise the organisation's management and employees;

- Monitor compliance;

- Assign responsibilities, raise awareness, provide training and conduct internal audits;

- Provide advice where requested and carry out Privacy Impact Assessments;

- Cooperate fully with the Data Protection Commission;

- Act as the contact point for the Commission, the authorities, the Data Subject and the public.

Towards Healing Data Loss Notification Procedure

Introduction:

The purpose of this document is to provide a concise procedure to be followed in the event that Towards Healing becomes aware of a loss of personal data. This includes obligations under law, namely the Data Protection Act (1988), and the Data Protection (Amendment) Act (2003) and European Union General Data Protection Regulation (EU GDPR) (May 2018)

The procedure is consistent with the guidelines issued by the Irish Data Protection Commission and is enshrined in Irish law.

Rationale:

The response to any breach of personal data (as defined by the legislation) can have a serious impact on Towards Healing's reputation and the extent to which the public Towards Healing as trustworthy.

Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification. This guide is to assist staff in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Scope:

The policy covers both personal and sensitive personal data held by Towards Healing. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by Towards Healing. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request procedure, the Data Retention and Destruction Policy and the Data Retention Periods List.

What constitutes a breach, potential or actual?

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on pc's and applications
- Emailing incorrect person
- Emailing a list of names to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to Towards Healing's Data Protection Officer or one of the Assistants.

Any employee who becomes aware of a likely data breach and fails to notify the the DPO will be subject to Towards Healing's disciplinary procedure.

A team comprising of the DPO, two Assistants and one other relevant member of staff will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commission and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances Towards Healing may (e.g. if required by the Office of the Data Protection Commission), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. Towards Healing will make recommendations to the data subjects which may minimise the risks to them. Towards Healing will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

Towards Healing is obliged to disclose any incident where the data is exposed to risk, even where the data may not have been disclosed outside the organisation or to an unauthorised individual

Information should be provided on the following aspects of the incident:

- A description of nature of the personal data breach;
- The categories and approximate number of Data Subjects concerned;
- The categories and approximate number of data records concerned;
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to be taken by Towards Healing to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

When will the Office of the Data Protection Commission be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commission by the DPO. There are no exceptions to this policy when the data subjects have already been informed, where the loss affects all Data Subjects, all incidents which expose personal or sensitive personal data to risk must be recorded and the Data Protection Commission notified.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commission is notified by the DPO only where the data on such devices is not encrypted immediately.

Data Loss Incident logging.

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commission. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commission was not informed. Such records will be provided to the Office of the Data Protection Commission upon request by the DPO.

Data Protection Incident Log

Data Protection Incident Log

Towards Healing DPO:

Log Date	Incident Description	Manual/ Automated?	Personal/ Sensitive?	Encrypted?	Volume of Records	Incident Mgr.	DPC Notified?	Notification Date	Additional Reference material

Breach Notification Process Under the GDPR

From 25th May 2018, the General Data Protection Regulation (GDPR) introduces a requirement for organisations to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. Organisations must do this within72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay.

Please see guidance below in relation to notifying this Office of a breach. Please note the separate reporting requirements that is applicable to providers of publicly available electronic communications networks or services, under the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011).

To facilitate decision-making and determine whether or not your organisation needs to notify the relevant supervisory authority and affected individuals, you should have a high-quality risk management process and robust breach detection, investigation and reporting processes.

Please note even where you determine there is no risk to affected individuals following a personal data breach, you need to keep an internal record of the details, the means for deciding there was no risk, who decided there was no risk and the risk rating that was recorded.

Initial notification of a breach

- All breach notification forms must be emailed to: breaches@dataprotection.ie
- All national breach notifications must be notified using the 'National Breach Notification Form'.
- All cross-border personal data breaches must be notified using the 'Cross-Border Breach Notification Form'.
  Cross-border processing means either:
    - Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of an organisation; or
    - Processing of personal data which takes place in the context of the activities of a single establishment of an organisation that substantially affects or is likely to substantially affect data subjects in more than one Member State
- **Note for providers of publicly available electronic communications networks or services:** Because the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) place specific obligations on providers of publicly available electronic communications networks or services to safeguard the security of their services, to report a breach on behalf of any organisation in this sector, please complete our Telecoms/ISP providers Data Security Breach Notification Form, available at the dataprotection.ie/secur-breach/
- In the subject line of the email please include the following information:

- Whether the breach you wish to notify DPC of is 'new' or an 'update' to a previous breach notification
- Your organisation name
- Your self-declared risk rating for the breach

An example of an email subject line is provided below:
Subject: New Breach Report, [organisation name], High Risk

Self-Declared Risk Rating

In determining how serious you consider the breach to be for affected individuals, you should take into account the impact the breach could potentially have on individuals whose data has been exposed. In assessing this potential impact, you should consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed. The levels of risk are further defined below:

- Low Risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
- Medium Risk: The breach may have an impact on individuals, but the impact is unlikely to be substantial
- High Risk: The breach may have a considerable impact on affected individuals
- Severe Risk: The breach may have a critical, extensive or dangerous impact on affected individuals.

Updating an existing notification

- If your notification was incomplete for any reason, you should submit further information when it becomes available. In this case, please submit a new version of the appropriate form with the relevant fields of the form completed.
- For updated notifications please include the following information in the subject line of the email:
    - Updated Breach Notification
    - Organisation Name
    - DPC reference number (if one has been provided)
    - The self-declared risk rating for the breach

An example of an email subject line is provided below:

Subject: Update Breach Report, [Organisation Name], [Reference Number], High Risk

Please do not include the personal information of affected individuals in your notification.

BREACH NOTIFICATION GUIDANCE UNDER THE DATA PROTECTION ACTS 1988-2003

If your organisation has experienced a personal data breach that occurred prior to 25th May 2018, and where the breach is not still ongoing after 25th May 2018, it is likely to be dealt with under the previous legislative regime. The relevant pieces of primary legislation in this regard are the Data Protection Acts 1988-2003 ("the Acts").

Under the provisions of the Acts, the DPC approved a personal data security breach Code of Practice to help organisations to react appropriately when they become aware of breaches of security involving customer or employee personal information. The Code of Practice does not apply to providers of publicly available electronic communications networks or services. This is because the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) place specific obligations on providers of publicly available electronic communications networks or services to safeguard the security of their services.

Applying the Personal Data Security Breach Code of Practice

Data controllers confronted with a breach of security affecting personal data should study the Code of Practice carefully. Some key considerations in relation to the application of the terms of the Code are set out below.

Paragraph one of the Code of Practice sets out the legal obligation to process personal data fairly and to take appropriate security measures to protect it.

Paragraph two refers to the need to focus on the rights of individuals where their personal data has been put at risk.

Paragraph three states that data controllers which have experienced an incident giving rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data must give immediate consideration to notifying the affected individuals. As the Code states, "this permits data subjects to consider the consequences for each of them individually and to take appropriate measures." The consequences may include the potential for fraud / identity theft, but it may also involve the potential for damage to reputation, public humiliation or even threats to physical safety. The Data Protection Acts give individuals the right to exercise control over how their data is used. A breach of personal data security may compromise that right. Notifying individuals is a remedial measure intended to redress the balance and restore some measure of knowledge and control. The information communicated to individuals should include information on the nature of the personal data breach and a contact point where more information can be obtained. It should recommend measures to mitigate the possible adverse effects of the personal data breach. If the affected individuals are not immediately identifiable, public notification may be the most appropriate means of communication, for example through the media or through a website. Data controllers should consider whether the method of notification adopted might increase the risk of harm to the data subjects.

Paragraph three of the Code also advises that data controllers should provide affected individuals with details of bodies that may be in a position to assist them, for example An Garda and financial institutions. Depending on the circumstances, other examples could include IT experts that can offer containment advice or internet companies that may assist in removing relevant cached links from their search engines. As with all other aspects of the Code, the DPC is happy to offer advice in this regard.

Paragraph four notes that there may be circumstances where a data controller may reasonably conclude that there is no risk to personal data due to the adoption of high-quality technological measures that effectively make the data inaccessible. For example, personal data stored on an encrypted laptop with secure access controls may be considered inaccessible in practice and the DPC considers that the loss of such a device would not normally involve a risk to the personal data stored on it. However the strongest encryption software [1] is useless if the access password is stored with the device or if the password is weak [2]. Other access controls (such as biometric identifiers, swipe cards, tokens etc.) may further strengthen security, particularly when used in combination with a complex password.

Paragraph five of the Code of Practice states that a data processor must report breaches of personal data security to the relevant data controller as soon as they become aware of the incident. This duty should be reflected in appropriate contracts signed between data controllers and data processors. The data controller should then follow the steps set out in the Code.

Paragraph six of the Code of Practice states that all incidents in which personal data has been put at risk should be reported to the DPC. The only exceptions are when the individuals have already been informed and the loss affects no more than 100 data subjects and the loss involves only non-sensitive, non-financial personal data. It should be noted that the fact that a data controller has notified the DPC of a loss of control of personal data does not necessarily imply that a breach of the Data Protection Acts 1988 and 2003 has taken place. The Code also makes clear that if a doubt exists - especially whether the technological measures protecting the data are such as to permit a reasonable conclusion that the personal data has not been put at risk - the matter should be reported to the DPC.

Paragraph seven of the Code of Practice sets a timeframe of two days for a data controller to inform the DPC once the data controller has become aware that personal data has been put at risk. Complex personal data security breach incidents may take a considerable period of time to fully investigate and resolve. All that is required is initial contact with the Office describing the facts as they are known and the steps being taken to address those facts. Personal data should not be included in such reports to the DPC and it is a matter for the data controller to decide the most secure method of contact, based on the nature of the information to be imparted.

Paragraph eight of the Code of Practice sets out the elements to be included in any formal report that may be sought by the DPC. The elements set out in paragraph eight should also be considered when preparing to notify data subjects directly of a personal data security breach incident. The Office may

seek other documents in addition based on the circumstances surrounding the incident. The Office will also set a timeframe for the delivery of a detailed report based on the nature of the incident and extent of the information required.

Paragraph nine of the Code of Practice states that the DPC may launch a detailed investigation depending on the nature of the personal data security breach incident. Such investigations may produce a list of recommendations for the attention of the relevant data controller. Responsible data controllers cooperate willingly with the DPC's investigations and are happy to comply with any recommendations he may issue. However, in rare cases in which such compliance is not forthcoming, the DPC may use its legal powers to compel appropriate actions.

Even if the DPC is not notified, **paragraph ten** of the Code of Practice states that data controllers should keep centrally a brief summary record of each personal data security breach incident with an explanation of the basis for not informing the DPC.

Paragraph eleven of the Code of Practice is self-explanatory, stating simply that the Code applies to all categories of data controllers and data processors to which the Data Protection Acts apply.

"Prevention is better than Cure"

Complying with the relevant reporting requirements following a data security breach is no substitute for the proper design of systems to secure personal data from accidental or deliberate disclosure. Our general advice on data security is here. But we accept that, even with the best-designed systems, mistakes can happen. As part of a data security policy, an organisation should anticipate what it would do if there were a data breach.
Some questions you might ask yourself:

- What would your organisation do if it had a data breach incident?
- Have you a policy in place that specifies what a data breach is? (It is not just lost USB keys/disks/laptops. It may include any loss of control over personal data entrusted to organisations, including inappropriate access to personal data on your systems or the sending of personal data to the wrong individuals).
- How would you know that your organisation had suffered a data breach? Does staff at all levels understand the implications of losing personal data?
- Has your organisation specified whom staff tell if they have lost control of personal data?
- Does your policy make clear who is responsible for dealing with an incident?
- Does your policy meet the requirements of the Data Protection Commissioner's approved Personal Data Security Breach Code of Practice?

If you wish to notify us that your organisation has experienced a breach of personal data that occurred prior to 25th May 2018,

please also do so using the relevant breach notification form provided above.

[1] the standard of encryption required to adequately secure data changes with advances in technology. Whole-disk encryption of 256-bit strength should meet the requirement at present.

[2] a strong password would typically be 14 characters long, contain a random selection of letters, numbers and symbols and be impossible to guess.

Personal Data Security Breach Code of Practice

1. The Data Protection Acts 1988 and 2003 impose obligations on data controllers [1] to process personal data entrusted to them in a manner that respects the rights of data subjects to have their data processed fairly (Section 2(1)). Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1)(d)).

This Code of Practice does not apply to providers of publicly available electronic communications networks or services. [2]

2. This Code of Practice addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. The focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.

3. Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected. [3] Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

4. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

5. All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

6. All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and** it affects no more than 100 data subjects **and** it does not include

sensitive personal data or personal data of a financial nature.[4]In case of doubt - in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner.

7. Data controllers reporting to the Office of the Data Protection Commissioner in accordance with this Code should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data. The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

8. Should the Office of the Data Protection Commissioner request a data controller to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

   - the amount and nature of the personal data that has been compromised;
   - the action being taken to secure and / or recover the personal data that has been compromised;
   - the action being taken to inform those affected by the incident or reasons for the decision not to do so;
   - the action being taken to limit damage or distress to those affected by the incident;
   - a chronology of the events leading up to the loss of control of the personal data; and the measures being taken to prevent repetition of the incident.

9. Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where a data controller has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

10. Even where there is no notification of the Office of the Data Protection Commissioner, the data controller should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

11. This Code of Practice applies to all categories of data controllers and data processors to which the Data Protection Acts 1988 and 2003 apply.

Document Retention and Destruction Policy

1. Policy and Purposes

This Policy represents the policy of Towards Healing with respect to the retention and destruction of documents and other records, both in hard copy and electronic media (which may merely be referred to as “documents” in this Policy). Purposes of the Policy include

- retention and maintenance of documents necessary for the proper functioning of Towards Healing as well as to comply with applicable legal requirements;
- destruction of documents which no longer need to be retained; and
- guidance for the Board of Directors, officers, staff and other constituencies with respect to their responsibilities concerning document retention and destruction.

Notwithstanding the foregoing, Towards Healing reserves the right to revise or revoke this Policy at any time.

2. Administration

2.1 Responsibilities of the Data Protection Officer

Towards Healing DPO shall be the administrator (“Administrator”) in charge of the administration of this Policy. The DPO’s responsibilities shall include supervising and coordinating the retention and destruction of documents pursuant to this Policy and particularly the Document Retention Schedule included below.

The DPO shall also be responsible for documenting the actions taken to maintain and/or destroy organisation documents and retaining such documentation.

The DPO may also modify the Document Retention Schedule from time to time as necessary to comply with law and/or to include additional or revised document categories as may be appropriate to reflect organisational policies and procedures.

The DPO is also authorised to periodically review this Policy and Policy compliance with legal counsel and to report to the Board of Directors as to compliance.

The DPO along with the Clinical Director and the Chief Executive Officer will assist in carrying out the DPO’s responsibilities, with the DPO, however, retaining ultimate responsibility for administration of this Policy.

2.2 Responsibilities of Constituencies.

This Policy also relates to the responsibilities of board members, staff, outsiders with respect to maintaining and documenting the storage and destruction of the organisation’s documents.

The DPO shall report to the Board of Directors (the board members acting as a body), which maintains the ultimate direction of management.

Towards Healing staff shall be familiar with this Policy, shall act in accordance therewith, and shall assist the DPO as requested, in implementing it.

Vendors or other service providers, depending upon the sensitivity of the documents involved with the particular outsider relationship, Towards Healing, through the DPO, shall share this Policy with the outsider, requesting compliance.

In particular instances, the DPO may require that the contract with the outsider specify the particular responsibilities of the outsider with respect to this Policy.

3. Suspension of Document Destruction; Compliance.

Towards Healing becomes subject to a duty to preserve (or halt the destruction of) documents once litigation, an audit or a government investigation is reasonably anticipated. Further, Government law imposes criminal liability (with fines and/or imprisonment) upon whomever "knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of Ireland or in relation to or contemplation of any such matter or case." Therefore, if the DPO becomes aware that litigation, a Governmental audit or a Government investigation has been instituted, or is reasonably anticipated or contemplated, the DPO shall immediately order a halt to all document destruction under this Policy, communicating the order to all affected constituencies in writing.

The DPO may thereafter amend or rescind the order only after conferring with legal counsel. If any board member or staff member becomes aware that litigation, a governmental audit or a government investigation has been instituted, or is reasonably anticipated or contemplated, with respect to the organisation, and they are not sure whether the DPO is aware of it, they shall make the DPO aware of it.

Failure to comply with this Policy, including, particularly, disobeying any halt Order, could result in possible civil or criminal sanctions. In addition, for staff, it could lead to disciplinary action including possible termination.

4. Electronic Documents; Document Integrity.

Documents in electronic format shall be maintained just as hard copy or paper documents are, in accordance with the Document Retention Schedule. Due to the fact that the integrity of electronic documents, whether with respect to the ease of alteration or deletion, or otherwise, may come into question, the DPO shall attempt to establish standards for document integrity, including guidelines for handling electronic files, backup procedures, archiving of documents, and regular check-ups of the reliability of the system; provided, that such standards shall only be implemented to the extent that they are reasonably attainable considering the resources and other priorities of Towards Healing.

5. Privacy.

It shall be the responsibility of the DPO, after consultation with Counsel, to determine how privacy laws will apply to the Towards Healing's documents from and with respect to employees and other constituencies; to establish reasonable procedures for compliance with such privacy laws; and to allow for their audit and review on a regular basis.

6. Emergency Planning.

Documents shall be stored in a safe and accessible manner. Documents which are necessary for the continued operation of the organisation in the case of an emergency shall be regularly duplicated or backed up and maintained in an off-site location.

The DPO shall develop reasonable procedures for document retention in the case of an emergency.

7. Document Creation and Generation.

The DPO shall discuss with staff the ways in which documents are created or generated. With respect to each employee or organisational function, the DPO shall attempt to determine whether documents are created which can be easily segregated from others, so that, when it comes time to destroy (or retain) those documents, they can be easily culled from the others for disposition.

For example, on an employee-by-employee basis, are e-mails and other documents of a significantly non-sensitive nature so that they might be deleted, even in the face of a litigation hold with respect to other, more sensitive, documents? This dialogue may help in achieving a major purpose of the Policy -- to conserve resources -- by identifying document streams in a way that will allow the Policy to routinely provide for destruction of documents.

Towards Healing has created and archive documents in a way that can readily identify and destroy documents with similar expirations.

Document Retention Schedule.

Document Type	Retention Period
Accounting and Finance	
Accounts Payable	7 years
Accounts Receivable	7 years
Annual Financial Statements and Audit Reports	Permanent
Bank Statements, Reconciliations & Deposit Slips	7 years
Credit Card Receipts	3 years
Employee/Business Expense Reports/Documents	7 years
Interim Financial Statements	7 years
Clinical	
Therapist Contracts	7 years
Clinical notes & information	7 years
Contributions/Gifts/Grants	
Contribution Records	Permanent
Grant Records	7 yrs after end of grant
Corporate and Exemption	
Articles of Incorporation and Amendments	Permanent
Bylaws and Amendments	Permanent
Minute Books, including Board & Committee Minutes	Permanent
Other Corporate Filings	Permanent
Revenue documentation	Permanent
Licenses and Permits	Permanent
Correspondence and Internal Memoranda	
Hard copy correspondence and internal memoranda relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate.	
Hard copy correspondence and internal memoranda relating to routine matters with no lasting significance	Two years

Correspondence and internal memoranda important to the organisation or having lasting significance	Permanent, subject to review

Employment, Personnel and Pension

Personnel Records	10 yrs after employment ends
Employee contracts	10 yrs after termination
Retirement and pension records	Permanent

Insurance

Property, D&O, Workers' Compensation and General Liability Insurance Policies	Permanent
Insurance Claims Records	Permanent

Legal and Contracts

Contracts, related correspondence and other supporting documentation	10 yrs after termination
Legal correspondence	Permanent

Management and Miscellaneous

Strategic Plans	7 years after expiration
Disaster Recovery Plan	7 years after replacement
Policies and Procedures Manual	Current version with revision history

Property – Real, Personal and Intellectual

Property deeds and purchase/sale agreements	Permanent
Property Tax	Permanent
Personal Property Leases	10 years after termination
Trademarks, Copyrights and Patents	Permanent

Tax

Tax exemption documents & correspondence	Permanent
Revenue Rulings	Permanent
Annual information returns –	Permanent
Tax returns	Permanent

Email Retention Policy

When Towards Healing looked at its outgoing and incoming emails and with the GDPR, and the real value to the organization a policy which meets the requirements and overcomes the challenges and review frequently to ensure it is up to date not just in terms of regulation, but also in terms of technology, ease of access, and any change in business requirements to process that data.

- Towards Healing will keep staff and users aware of the policies and make sure they understand it fully.
- Towards Healing will continue to review the policies and test your access to archived data

- Following Methodology was implemented:

    - All incoming & outgoing emails to Data Subjects will be copied onto relevant profiles

        When a processor is emailing or in receipt of an email from a **client** regarding their service with Towards Healing, please ensure the email is entered on the client profile only

        When a processor is emailing or in receipt of an email from a **Therapist** about Portal, Insurance, Contract TATP, CP (how to fill in), please enter the email on therapist profile only.

        When a processor is emailing or in receipt of an email from a **therapist** about a **client,** please add the email on client profile only.

        If a number of clients are mentioned throughout an incoming or outgoing email to or from a **therapist,** please add relevant notes to **relevant client profiles.**

- All emails to be marked as “read”
- No “unread” emails to be held in Inbox on Outlook
- Any Banking emails or what appears to be junk, please mark as “junk” by right clicking on email, select “junk mail”.
- Clutter to be cleared daily
- Deleted emails to be cleared daily
- Archive off emails more than 1 year old on each user’s profile
- Erasure of emails that go past a two year (in archive), Towards Healing will use a certified, auditable tool so we can prove the process has be completed.

Electronic Mail (E-mail) to or from Towards Healing

Electronic mail (e-mails) relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document to which they relate but may be retained in hard copy form with the document to which they relate.

Electronically Stored Documents

Electronically stored documents (e.g., in pdf, text or other electronic format) comprising or relating to a particular document otherwise addressed in this Schedule should be retained for the same period as the document which they comprise or to which they relate but may be retained in hard copy form (unless the electronic aspect is of significance).

Electronically stored documents considered important to the organisation or of lasting significance should be printed and stored in a central repository (unless the electronic aspect is of significance). Permanent, subject to review

Electronically stored documents not included in either of the above categories
Two years

Towards Healing Privacy Policy (for website)

Towards Healing commitment to privacy

Towards Healing knows that you care how information about you is used and shared, and we appreciate you trusting that we will do so carefully and sensibly. To better protect your privacy, we provide this Privacy Policy explaining our practices and the choices you can make about the way your information is collected and used by Towards Healing. The information below explains our policy regarding your privacy, both online and offline. By visiting www.parentsplus.ie or sharing personal information with Towards Healing you are accepting the practices described in this Privacy Statement.

Our www.towardshealing.ie website is maintained by Towards Healing

What personally identifiable information is collected by Towards Healing?

When you visit our website, you may contact certain staff members (listed) with information such as - name, address, email address, telephone numbers that you knowingly choose to disclose, which is collected on an individual basis for various purposes. or simply asking a question. We receive and store any information you enter on our Database or give us in any other way, whether it is online or offline. We ask for personal information so that we can fulfil your request and return your message. This information is retained and used in accordance with existing laws, rules, regulations, and other policies.

Towards Healing does not collect personal information from you unless you provide it to us. If you choose not to provide any of that information, we may not be able to fulfil your request or provide services, but you will still be free to browse the other sections of our website owned and administered by Towards Healing. This means that you can visit our site without telling us who you are or revealing any personally identifiable information about yourself.

The way we use information

When you supply information about yourself for a specific purpose, we use the information for only that purpose (such as to provide the service or information you have requested). We do not share this information with outside parties except to the extent necessary to complete your request for services. In order to provide you service, Towards Healing request you contact the therapist to provide your first appointment.

We use return email addresses to answer the email we receive, to receipt any transactions or if follow-up for that specific function is required. Such addresses are carefully guarded by Towards Healing for their specific purpose and are not shared with outside parties. An individual's information is stored on a secure cloud system which we use to process data and keep in contact with you.

Towards Healing does not sell, rent, give-away or share its email addresses or other personal contact information with outside sources.

Should any material changes be made to the ways in which we use personally identifiable information, Towards Healing will take commercially reasonable measures to obtain written or email consent from you. We will also post the changes to our use of personally identifiable information on our website at least 30 days prior to a change.

Our commitment to data security

Personally, identifiable information is stored on our database which is a secure cloud system. It is not publicly accessible. Further, personally identifiable information is only accessed by Towards Healing personnel on a "need to know" basis. To prevent unauthorised access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect online. Towards Healing has data protection policies and procedures in place to ensure data security.

Your Choice and how you can Opt-out of communications

Therapists:
When Towards Healing send out "mass emails", there will be an option for our Processors (therapists) to "Opt in / Opt out". When "Opt out" is selected, Towards Healing will include "Do not Contact" on the profile. Information you submit to Towards Healing over the phone will not be used for this purpose unless you 'opt-in' specifically. "Opt out" will only be accepted following certain criteria (i.e. no active cases within 7-year period)

Clients:
If you have received services in previous years from Towards Healing and wish no longer to receive any further services, please use the following options to have your personal identifiable information nominalized.

- You can send an email to: dataprotection@towardshealing.ie
- You can send mail to the following address:
  Towards Healing, PO Box 5654, Dundrum, Dublin 14

How to correct/update your information

If you would like to verify the data we have received from you or to make corrections to it, you may contact us directly by requesting your information by letter and including an up to date copy of proof of identification.

Cookies

How does this site use cookies?

By using the site, you agree that we may store and access cookies on your device.

What does this mean?

Cookies are small text files held on your own computer. Cookies will never contain any personally identifiable information. We use cookies in order to deliver the best possible service to you, provide a secure and effective site service for clients.

What are cookies?

Cookies are small text files sent from websites and stored in the user's web browser while user is browsing a website.

When users visit the same website again, the browser sends cookies back to the website allowing the website to recognise the user and remember things like personalised details or preferences. More information about cookies and details of how to manage or disable them can be found on www.aboutcookies.org.

Towards Healing Cookie Policy

Towards Healing respects, the privacy of all visitors to our website. This Cookie Policy outlines our policy concerning the use of cookies on towardshealing.ie.

We may update our Cookie Policy from time to time to reflect any changes in technology or legislation which may affect the way in which cookies are used by us and how you as a user, can manage them.

Which cookies does Towards Healing use?

When you use the towardsdhealing.ie website the following types of cookies can be set on your device:

Strictly necessary cookies

Some examples of these cookies include Identifying you as being signed in and keeping you logged in throughout your visit. These cookies don't contain any personally identifiable information.

Website Performance cookies

These cookies are used to collect statistical information about visitors of the website and the pages they view. These cookies don't collect information that identifies a visitor. All information these cookies collect is aggregated and used anonymously. We use these cookies to understand what content is popular which helps us to improve our website.

For more information on how to manage cookies, including opt-out of performance cookies please visit: http://www.aboutcookies.org/Default.aspx?page=1

External Links on the website

This website contain links to other websites. Please note that when you click on one of these links, you are entering another site. We encourage you to read the privacy statements of these linked websites as their privacy policy may differ from ours. Towards Healing cannot be held responsible for content contained on external websites and these links are provided for information purposes only.

Changes to this privacy statement

Changing business practices and circumstances may require that we make changes to this privacy policy from time to time. Any changes will be reflected on this website. Towards Healing reserves the right to modify its website and/or this Privacy Policy at any time and visitors are deemed to be apprised of and bound by any such modifications. Our goal is to provide all services to visitors in an accessible, efficient and friendly manner while maintaining their privacy. If you have comments or questions regarding privacy, please contact us.

Legal Disclaimer

We may disclose personal information when required by law or in the good-faith belief that such action is necessary in order to conform to the edicts of the law or comply with legal process served on Towards Healing.

For more information

If you have any questions, concerns or comments about your privacy, please send us a description of your concern via email to dataprotection@towardshealing.ie

Closed Circuit Television System (CCTV)

Introduction

Closed Circuit Television Systems (CCTVS) was introduced in consultation with staff, management and the Board of Directors. The operation of the CCTV will be reviewed regularly in consultation with staff, management and the Board of Directors.

1. Purpose of Policy

"The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of St Joseph's Lodge, Mount ST Mary's, Dundrum, Dublin 14

CCTV systems are installed (both internally (in the hall) and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the staff, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at the Lodge is intended for the purposes of:

- protecting the building and assets, both during and after hours;
- promoting the health and safety of staff and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Gardai in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders;

2. Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where work and activities are carried out, Towards Healing will ensure that CCTV system, where installed, are operated only in a way that is compatible with the provisions of this policy.

3. General Principles

CCSS T/a Towards Healing as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, and invitees to its premises. CCSS T/a Towards Healing owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance

for the purpose of enhancing the quality of life by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Information obtained through the CCTV system may only be released when authorised by the Chief Executive Officer following consultation with the DPO and the Chairperson of the Board of Directors. Any requests for CCTV recordings/images from An Garda Síochána will be fully recorded and legal advice will be sought if any such request is made. (See "Access" below). If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be requested in writing and CCSS T/a Towards Healing will immediately seek legal advice.

CCTV monitoring for security purposes will be conducted in a manner consistent with all existing policies adopted by CCSS T/a Towards Healing including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of areas for security purposes within the premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of CCSS T/a Towards Healing

CCTV system and associated equipment will be required to be compliant with this policy following its adoption by CCSS T/a Towards Healing. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003 and EU GDPR May 2018.

4. Justification for use of CCTV

Section 2(1)(c)(iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that *CCSS T/a Towards Healing* needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the outside of St Joseph's Lodge has been deemed to be justified by management. The system is intended to capture images of intruders or of individuals damaging property, harassing staff or removing goods without authorisation.

CCTV systems will not be used to monitor normal day-to-day work.

In other areas of the premises where CCTV has been installed, e.g. hallway, management have demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

5. Location of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. *CCSS T/a Towards Healing* has endeavoured to select locations for the installation of CCTV cameras, which are least intrusive to protect the privacy of individuals. Cameras placed to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

Camera Locations General Surveillance / Monitoring

- Gable end
- Viewing door
- Corner looking towards residence
- Viewing rear path
- End Gable Viewing
- Internal Viewing Hall

CCTV Video Monitoring and Recording of Public Areas may include the following:

- ***Protection of St Joseph's Lodge and property:*** The building's perimeter, entrances and exits.
- ***Monitoring of Access Control Systems:*** Monitor and record restricted access areas at entrances to buildings and other areas
- ***Verification of Security Alarms:*** Intrusion alarms, exit door controls, external alarms
- ***Video Patrol of Public Areas:***, Main entrance to premises
- ***Criminal Investigations (carried out by An Garda Síochána):*** Robbery, burglary and theft surveillance

6. Covert Surveillance

CCSS T/a Towards Healing will not engage in covert surveillance.

Where An Garda Síochána requests to carry out covert surveillance on premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by An Garda Síochána will be requested in writing and the premises will seek legal advice.

7. Notification Signage

The CEO will provide a copy of this CCTV Policy on request to staff and visitors to the premises. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Board of Directors. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to St. Joseph's Lodge. Signage shall include the name and contact details of the Data Controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

WARNING
CCTV cameras in operation
Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying & harrassment, for the safety of our staff and visitors and for the protection of St Joseph's Lodge property. This system will be in operation 24 hours a day, every day. These images may be passed to An Garda Síochána.
This scheme is controlled by CCSS T/a Towards Healing, and operated by Mark Wilson Security Systems
For more information, contact *Breda Flood 087-2613301*

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors,
- at or close to each internal camera

8. Storage & Retention

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. Towards Healing needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the CEO. The CEO may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Gardai, the management, When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

9. Access

Tapes/DVDs storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Management.

In relevant circumstances, CCTV footage may be accessed:

- By An Garda Síochána where CCSS T/a Towards Healing are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on CCSS T/a Towards Healing property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To assist the CEO in establishing facts in cases of unacceptable behaviour, in which case, staff will be informed; or
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to CCSS T/a Towards Healing or
- To individuals (or their legal representatives) subject to a court order.

- To CCSS T/a Towards Healing insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Requests by An Garda Síochána: Information obtained through video monitoring will only be released when authorised by the CEO following consultation with the Chairperson of the Board of Directors. If An Garda Síochána request CCTV images for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be made in writing and CCSS T/a Towards Healing should immediately seek legal advice.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to CCSS T/a Towards Healing Data Protection Officer. Response to such a request and must respond **within 30 days.**

Access requests can be made to the following: Data Protection Officer, Towards Healing, PO Box 5654, Dundrum Rd., Dublin 14

A person should provide all the necessary information to assist CCSS T/a Towards Healing in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the organisation.

In giving a person a copy of their data, CCSS T/a Towards Healing may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

10. Responsibilities

The CEO, following consultation with the DPO, will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by CCSS T/a Towards Healing
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within CCSS T/a Towards Healing
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at CCSS T/a Towards Healing is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy

- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. *NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána].*
- Give consideration to both staff and visitors feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the organisation and be mindful that no such infringement is likely to take place
- Co-operate with the Health & Safety Officer of CCSS T/a Towards Healing in reporting on the CCTV system in operation in the school
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chairperson of the Board of Directors.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- Ensure that where An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chairperson of the Board of Directors.

11. Security Companies

The CCTV system is controlled by a security company contracted by the CCSS T/a Towards Healing. The following applies:

CCSS T/a Towards Healing has **a written contract with the security company in place** which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply. The written contract also states that the security company will give CCSS T/a Towards Healing all reasonable assistance to

deal with any subject access request made under section 4 Data Protection Acts 1988 and 2003 which may be received by the school within the statutory time-frame (30 days).

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients). Sections 2(2) and 2C of the Data Protection Acts place a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company have been made aware of their obligations relating to the security of data. See Content of the Service Agreement for further guidance.

12. Implementation & Review

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commission, An Garda Síochána, Charities Act., legislation and feedback from staff and visitors.

The date from which the policy will apply is the date of adoption by the Board of Directors. Implementation of the policy will be monitored by the CEO

Towards Healing Threshold

Towards Healing holds very sensitive data, our threshold is high, the following needs to be adhered to on a daily basis by all.

Clear Desk Policy

Is your desk clear when you leave the office ?

No documentation with client / therapist names, records and telephone numbers are to be left on desks. All information should be locked away.
On any occassion, where official papers are found, this will be retained in a secure location and any action to be taken will be considered by the DPO (Data Controller)

Equiptment

Computers :

Lock and log off your computer when finished working and at the close of your shift

Lock computer screen when you leave your desk at all times.

Passwords

All passwords to Salesforce are unique to each user and are updated regularly.

If asked at any time by the computer to save your password, please answer **NO**. A new password will be forwarded to you, please keep it safe and pass on to your Line Manager.

All access to Salesforce is through Firefox, and not Internet Explorer

Laptops

Laptops which are the property of Towards Healing are only to be used by employed staff.

Access to Towards Healing files are prohibited outside the office unless through Laptop supplied by Towards Healing

Access to Towards Healing emails are also prohibited from outside the office

Are you the only one accessing the laptop ?

Keys

All members of staff have been issued with keys for offices and presses. Ensure after your shift all presses are locked where sensitive data is stored.

Keys of presses or of the buildings are not to be left in the door or on the desk at any time

Encriptions

Towards Healing has incorporated Encrytion on all sensitive data held on client profiles and also when emailing therapists and civil authorities.

All documentation to be stored on the Q Drive (Office 365) and not on Desktops.

Shredders

Shredders are in place in Room 2 of St Joseph Lodge for paper to be shredded
and
Room 1 of the Big House for documents relating to DPO, CEO, Financial, Administration and Advocacy.

Please ensure paper (for no further use) is shredded before you leave the office and that no documentation is left in bins or on desks.

Self-help checklist on Data Protection Policy – (to be added to Employee Handbook)

Remember you should be able to answer YES to all of the questions below. If you can, Towards Healing is in good shape from a Data Protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

MAIN RESPONSIBILITIES

Rule 1: Lawful, Fair and Transparent Processing

- At the time when we collect information about individuals, are they made aware of the uses for that information?
- Are people made aware of any disclosures of their data to third parties?
- Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them
- Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Specified and Lawful Purpose

- Are we clear about the purpose (or purposes) for which we keep personal information?
- Are the individuals on our database also clear about this purpose?
- If we are required to register with the Data Protection Commissioner, does our register entry include a proper, comprehensive statement of our purpose? *[Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]*
- Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Minimisation of Processing

- Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?
- Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?
- If an individual asked us to justify every piece of information we hold about him or her, could we do so?

Rule 4: Accuracy

- Do we check our data for accuracy?
- Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?
- Do we take steps to ensure our databases are kept up-to-date?

Rule 5: Storage Limitation

- Is there a clear statement on how long items of information are to be retained?
- Are we clear about any legal requirements on us to retain data for a certain period?
- Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?
- Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 6: Security and Confidentiality

- Are there defined rules about the use and disclosure of information?
- Are all staff aware of these rules?
- Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.
- Is there a list of security provisions in place for each data set?
- Is someone responsible for the development and review of these provisions?

Rule 7: Liability and Accountability

- Are these provisions appropriate to the sensitivity of the personal data we keep?
- Are our computers and our databases password-protected, and encrypted if appropriate?
- Are our computers, servers, and files securely locked away from unauthorised people?

Rule 8: The Right of Access

- Is a named individual responsible for handling access requests?
- Are there clear procedures in place for dealing with such requests?
- Do these procedures guarantee compliance with the Act's requirements?