

One in Four Ireland CLG

Data Protection Policy

Document Control	
Authorised by:	Management Team One in Four
Date:	25 th May 2018
Review Date:	25 th Nov 2018
Drafted by:	Deirdre Mackay
Document Version	1.00
Document Review History	
Previous Document:	N/A
Previous Version:	N/A
Amended (Y/N):	N/A

Contents

Part 1: Policy	3
1.1 Policy Introduction	3
1.2 The Eight Data Protection Principles	3
1.3 Policy Statement	4
1.4 Policy Purposes	4
1.5 Policy Scope	4
1.6 Descriptions/Definitions	5
Part 2: General Guidelines	7
2.1 Introduction	7
2.2 Obtain and process information fairly	7
2.3 Keep personal data only for one or more specified, explicit and lawful purposes	9
2.4 Use and disclose data only ways compatible with the purposes for which it was given	9
2.5 Keep data safe a secure	10
2.6 Keep personal data accurate, complete and up-to-date	11
2.7 Ensure personal data is accurate, relevant and non-excessive	11
2.8 Retain personal data for no longer than it necessary for the purpose(s) for which it was processed	12
2.9 Provide a copy of an individual’s personal data upon request	12
2.10 Consent to images or audio being recorded or processed	13
Part 3: Risk Management & Compliance Audits	13
3.1 Internal Compliance	13
3.2 External Compliance	14
3.3 Data Protection / Privacy Impact Assessments	14
Part 4: Information & Data Access Requests & Retention	15
4.1 Information Request (Section 3 request)	15
4.2 Access Request (Section 4 request)	16
4.3 Exemptions to providing data in response to an Access Request	17
4.4 Correcting Data	18
4.5 Data Retention Policy	18
Part 5: Data Breach Management	20
5.1 Introduction	20
5.2 Management of a Data Breach in One in Four Ireland CLG	20

5.2.1	Incident Reporting	21
5.2.2	Notification of Data Breach & Risk Assessment (Internal).....	21
5.2.3	Notification of Data Breach & Risk Assessment (External)	22
5.2.4	What Constitutes a ‘Notifiable Breach’?.....	23
5.2.5	Data Protection Commissioner’s role following a Notifiable Breach	24
5.2.6	Evaluation Response	24
Part 6: Awareness Training & Support for Staff		25
6.1	Introduction	25
6.2	Data Protection Awareness Training	25
6.3	Data Protection Support	25
Conclusion		26
Annex 1: Health & Safety matters.....		27
	Accidents/Injuries	27
	Data retention relating to certain accidents.....	27
	Sick Leave/Medical Certificates	27
Annex 2: Updates.....		29
	Relevant guidance notes and press releases from the Data Protection Commissioner and Office of the Data Protection Commissioner.....	29

Part 1: Policy

1.1 Policy Introduction

This policy was drafted on foot of review of policies and data in advance of the GDPR introduction.

At time of writing, the Data Protection Acts 1988 & 2003 govern all matters relating to data protection.

The EU General Data Protection Regulations (GDPR) will come into force on the 25th of May 2018.

This Data Protection Policy will be reviewed in 6 months in November 2018.

1.2 The Eight Data Protection Principles

Under the Data Protection Acts 1988 & 2003, One in Four Ireland CLG (as a 'data controller') has a legal responsibility to:

1. Obtain and process data fairly.
2. Keep personal data for one or more specified and lawful purposes.
3. Only process personal data in ways compatible with the purposes for which the personal data was given to One in Four Ireland CLG
4. Keep personal data safe and secure.
5. Keep personal data accurate and up-to-date.
6. Ensure that personal data is adequate, relevant and not excessive.
7. Retain personal data no longer than is necessary for the specific purpose (or purposes) for which the data was given.
8. Provide a person who requests it a copy of their personal data in accordance with the Acts.

1.3 Policy Statement

One in Four Ireland CLG. is a 'data controller' as defined by the Data Protection Act and endeavours to:

- Comply with the Data Protection Acts and best practice.
- Comply with the eight principles of data protection.
- Protect the privacy rights of individuals whose data we process.
- Ensure that personal data in the possession of One in Four Ireland CLG is kept safe and secure.
- Support staff to meet their legal responsibilities as set out under the eight data protection principles.
- Respect individual's rights, regardless of who they are.
- Provide awareness, adequate training and support for staff that process personal data.

1.4 Policy Purposes

The purposes of this of this Data Protection policy are to:

- Outline how One in Four Ireland CLG endeavours to comply with the Data Protection Acts.
- To provide good practice guidelines for staff.
- To reduce the risk of and protect against any breach of the Data Protection Acts by One in Four Ireland CLG
- To be prepared to answer any queries or address any concerns by the Data Protection Commissioner should they arise.
- To ensure that individuals are able to access their personal data upon request.

1.5 Policy Scope

This Data Protection Policy applies to all staff, employees and or volunteers of One in Four Ireland CLG regardless of whether their role or job description requires or specifies any processing of personal data.

A public version of this policy, in the form of a Privacy Policy, will be made public on the company website (www.oneinfour.ie) for all individuals and it is separate to our Cookie Policy that is also available on the website.

This Data Protection Policy is internal to the company but may be made available to any relevant third party upon request as part of entering into or complying with any data processing agreement between One in Four Ireland CLG and a relevant third party.

1.6 Descriptions/Definitions

‘Access Request’ is where an individual makes a request to an organisation for a copy of their personal data under Section 4 of the Data Protection Acts.

‘Company’, or the ‘organisation’, means One in Four Ireland CLG

‘Data’ is any information that can be processed and includes automated data, manual data (including information connected with a ‘Relevant Filing System’) and electronic data.

‘Data Controller’ means a person (or company) who, either alone or with others, controls the contents and use of personal data. In a general context for the purposes of this policy, ‘data controller’ also refers to One in Four Ireland CLG

‘Data Processing’ is the performance of any operation in connection with the use of data, including:

- Obtaining, recording or storing data.
- Collecting, organising, altering or amending data,
- Retrieving or using data.
- Disclosing the data via transmission, dissemination, or the use of any method of communication or otherwise making the data available.
- Aligning, combining, blocking access to, erasing or destroying the data.

‘Data Processor’ means a person (or company) who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

‘Data Subject’ means an individual who is the subject of Personal Data.

‘Information Request’ is where an individual makes a request to an organisation as to whether an organisation has information about the individual, the description of the information and the purposes(s) for holding the information, under Section 3 of The Data Protection Acts.

‘Personal Data’ is data relating to a living individual who can be identified by the data or who can be identified with the data in conjunction with other information that is in the possession or, or will likely come into the possession of, the Data Controller. Personal data includes photos, phone calls, voice recordings and video recordings.

‘Relevant Filing System’ means any set of information relating to individuals in a set structured, either by reference to individuals or by reference to criteria related to individuals in such a way that specific information relating to a particular individual is readily accessible. For example, payroll software, customer relationship software, accounting software, etc.

‘Sensitive Personal Data’ means personal data relating to:

- a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
- b) whether the data subject is a member of a trade union,
- c) the physical or mental health or condition or sexual life of the data subject,
- d) the commission or alleged commission of any offence by the data subject, or,
- e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

‘The Data Protection Acts’ means the Data Protection Act 1998 and The Data Protection (Amendment) Act 2003.

Part 2: General Guidelines

2.1 Introduction

The Data Protection Acts protect the privacy rights of individuals and do so by placing obligations on anyone who use or processes personal data about a person. One in Four Ireland CLG is a data controller under the Acts and endeavours to meet its legal responsibilities and protect the privacy of all people who interact with the company. We do this by ensuring that we process all data in accordance with this Data Protection Policy.

Our staff, employees and volunteers have legal responsibilities relating to the processing of personal data and this policy is to help ensure they, and the company, protect themselves from any breaches of the Data Protect Acts and in doing so, uphold and protect individuals' privacy rights.

The obligation on One in Four Ireland CLG, and all staff, employees and volunteers, is to incorporate and apply the following eight Data Protection Principles, insofar as possible, into their working practices.

2.2 Obtain and process information fairly

To fairly obtain data the data subject must, at the time of the personal data being collected, be made aware of:

- a) The name of the data controller (which is One in Four Ireland CLG);
- b) The purpose(s) of collecting the data;
- c) The identity of any representative nominated for the purpose of the Acts (i.e. any Data Protection Officer, Data Processor, company point of contact for queries, etc.);
- d) Whether replies to questions asked are obligatory and the consequences of not providing replies to those questions (e.g. mandatory fields in order forms);
- e) The existence of the right to access of their personal data;
- f) The right to rectify their data if inaccurate or processed unfairly;
- g) Any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary so as to be aware as to their data will be processed;
- h) In circumstances where the personal data is not obtained from the data subject, e.g. via a third party, then the above information must be provided to the data subject and they must be informed as to the identity of the original data controller from whom the information was obtained (i.e. where the data came from) and the categories of data concerned. (This paragraph is currently being discussed with the Data Commissioner in light of the confidential nature of our work)

[Continued on the next page]

To **fairly process personal data** it must have been fairly obtained, and:

- the data subject must have given consent to the processing;
- or
- the processing must be necessary for one of the following reasons:-
 - the performance of a contract to which the data subject is a party;
 - in order to take steps at the request of the data subject prior to entering into a contract;
 - compliance with a legal obligation, other than that imposed by contract;
 - to prevent injury or other damage to the health of the data subject;
 - to prevent serious loss or damage to property of the data subject;
 - for the administration of justice;
 - to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged;
 - for the purpose of the legitimate interests pursued by One in Four Ireland CLG except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject

To **fairly process sensitive personal data** it must have been fairly obtained, and:

- In the case of marketing/fundraising, the data subject must have given explicit consent (or where they are unable to do so, for reasons of incapacity of age, explicit consent must be given by a parent or legal guardian) for the processing.
- or
- the processing must be necessary for one of the following reasons:-
 - for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
 - to prevent injury or other damage to the health or safety of the data subject or another person;
 - to prevent serious loss or damage to property of the data subject or another person,
 - for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights;
 - compliance with any legal obligation imposed by law;
 - for medical purposes in order to save life or injury to a person;
 - for the purposes of an assessment or payment of a tax liability;
 - for the purposes of an administration of a Social Welfare scheme.

2.3 Keep personal data only for one, or more specified, explicit and lawful purposes

A data subject has the right to question the purpose for which their data is being held and One in Four Ireland CLG must be able to identify that purpose when requested.

In order to comply with this requirement, employees should be aware:-

- that a person is entitled to know the specific reasons why their data is being processed;
- that the purpose for the processing of data is lawful;
- of the different categories of data which are held and the specific purpose of each category.

Employees should be able to provide the above information to data subjects upon request (via a 'information request' – see *Information Request*).

2.4 Use and disclose data only in ways compatible with the purposes for which it was given

Personal Data should only be used and disclosed in ways that are necessary or compatible with the original purpose for which it was obtained;

Staff are not to disclose any personal data to any third party without the consent of the data subject.

Personal information should not be disclosed to work colleagues unless they have a legitimate interest in the data in order to fulfil official employment duties.

There may be some circumstances or exemptions in which disclosure of data is mandated and or permitted under certain legislative provisions (e.g. Protected Disclosures Act, etc.). Employees are to refer to their employment contract and handbook for further details. Volunteers are to refer to their volunteers agreement for further details.

Personal data may be disclosed with the express consent of the data subject.

Personal data may be disclosed without the express consent of the data subject in the following circumstances:

Where the data subject has already been made aware of the person or organisation to whom the data may be disclosed,

- Where it is required by law;
- Where it is required for legal advice and or legal proceedings;
- Where it is required for the purpose of preventing detecting, investigating or in the prosecution or defence of an offence;
- Where it is urgently required to prevent injury to a person or severe loss or damage to property;

2.5 Keep data safe and secure

One in Four Ireland CLG strives towards high standards of security for all personal data. Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure, sharing or destruction of personal data; this includes protecting against any accidental loss, dissemination or destruction of data.

To protect personal data, One in Four Ireland CLG security includes the following practices and procedures;

- Access to central IT servers is restricted in a secure location to a limited number of staff, with appropriate procedures for the accompaniment of any non-authorised staff or contractors;
- Access to any personal data within the company is restricted to authorised staff for legitimate purposes only;
- Access to computer systems is password protected;
- Non-disclosure of personal security passwords to any individual other than designated individuals, i.e. Executive Director, PA to Executive Director, External IT Consultant and GDPR Responsible.
- Information on computer screens and manual files are kept out of sight from callers or visitors to company offices;
- Computer servers are backed up daily off site. A report is published daily and monitored by CEO, IT consultant and administrator.
- Company network is monitored by security software that is subject to ongoing review and certification by a professional software security company;
- Company network integrity is processed and documented via an external professional software security company;
- Personal manual data is securely held in locked cabinets, locked rooms and rooms with limited access with the only access restricted to staff who have a legitimate use for the secured data;
- Special care, including encryption, must be taken regarding the use, access, location and storage of any mobile computing device and storage devices, e.g. laptops, USB drives, etc.;
- Personal data is not to be stored on portable devices except in essential circumstances for short time use, for as briefly as possible. Where deemed essential, the data must be encrypted and deleted from the portable device as quickly as possible. Personal data is not to be stored long term in any removable, easy to use USB sticks or flashcards;
- All reasonable measures are to be taken to ensure that staff are made aware of company security measures and to comply with them;
- Any physical paper that contains personal data that is no longer necessary to be retained must be destroyed as soon as possible via appropriate shredding techniques using a suitable shredder (e.g. cross-cutting shredding).

2.6 Keep personal data accurate, complete and up-to-date

The company endeavours to support staff and any relevant parties by maintain records of personal information that are accurate, complete and up-to-date. Apart from being requirements of the Data Protection Acts, it is in the interests of One in Four Ireland CLG to ensure accurate data for reasons of efficiency and effective decision making.

As such, it is important to note that:

- Manual and computer procedures are suitable to maintain high levels of data accuracy;
- Departments should have regular review cycles or procedures to ensure information processed is accurate and up-to-date;
- Management and company officials ensure periodical reviews and auditing of procedures to ensure data processed is accurate and up-to-date;
- Where a data subject advises of any changes to their personal data, or any mistakes in their personal data, that the personal data is amended or destroyed as soon as possible;

2.7 Ensure personal data is accurate, relevant and non-excessive

One in Four Ireland CLG will only process the minimum amount of personal data that is necessary to achieve our purpose(s). In order to achieve this, Privacy Impact Assessments will be conducted for new processes and procedures to help reduce any data protection concerns.

For existing, and or ongoing, processes and procedures, information sought from data subjects must be:

- Adequate for the purpose(s) for which it is sought (i.e. required to fulfil the purpose);
- Relevant to the purpose(s) for which it was sought;
- Not excessive in relation to the purpose(s) for which it was sought.

There should be periodic reviews of the relevance of personal data sought from data subject through various company channels (e.g. website, contact forms, etc.) and periodic reviews as to the basis for any information, to ensure ongoing compliance.

2.8 Retain personal data for no longer than it necessary for the purpose(s) for which it was processed

Data should only be retained for the time necessary for the purpose(s) of which it was processed. As soon as the data is no longer necessary, it should be destroyed or deleted in an appropriate manner, subject to the following retention period.

The following is an edited overview of the company's data retention policy (see *Data Retention Policy*).

One in Four Ireland CLG has a personal data retention period of seven years based upon the general six year limitation period stated in the Statute of Limitations, plus one additional year to allow for service of legal proceedings, equating to seven years in total.

Exceptions to the above limitation period include:

- tax record and payroll records for taxation purposes that are subject to Revenue retention periods;
- Employment interviews and data relating to interview and selection of potential employees (e.g. CVs, cover letters, etc.) of which data relating to unsuccessful candidates will be retained for one year after the closing of the relevant selection period, or job interviewed, to allow service relating to any matter that may arise relating to the selection or employment process (e.g. access to employment under the Employment Equality Acts);
- Data that may assist in the reporting, investigation or litigation relating to a criminal that may reasonably affect the company.
- Any data which management deem appropriate under the circumstances to retain outside the standard seven year retention period, subject to regular reviews as to the necessity of retaining such data that will be destroyed once no longer required.
- Data relation to accidents that require a mandated investigation under the Health, Safety and Welfare at work legislation (see *Data Retention Policy*).

2.9 Provide a copy of an individual's personal data upon request

An individual is entitled to find out whether an organisation has information about the individual, the description of the information and the purposes(s) for holding the information, under Section 3 of The Data Protection Acts.

Please see *Information Requests* as to how to process an information request under Section 3 of the Data Protection Acts.

An individual is entitled to get a copy of their personal data that an organisation may hold about that individual under Section 4 of the Data Protection Acts.

Please see *Access Requests* as to how to process an access request under Section 4 of the Data Protection Acts.

2.10 Consent to images or audio being recorded or processed.

A person can be identified via their image or voice so any image, visual recording (with or without sound) or any audio recording (with or without images) constitutes personal data and are subject to the Data Protection Acts.

In circumstances where any audio or visual image is recorded or processed relating to medical data the **explicit** consent of an individual is required with an exception being any statutory provision requiring the preservation of any audio or visual images. For example, the Safety, Health and Welfare at Work (Reporting of Accidents and Dangerous Occurrences) Regulations 2016 (S.I. No. 370 of 2016) mandates that the company must report and investigate certain accidents in the workplace.

Part 3: Risk Management & Compliance Audits

3.1 Internal Compliance

One in Four Ireland CLG endeavours to protect the privacy of all data subjects, including customers, suppliers and employees.

We do this by appointing a single point of contact within the company for all data protection related matters. The single point of contact is Deirdre Mackay.

Version 1.00 was drafted on foot of an internal data protection audit overseen by senior management. The company undertakes to review this data protection policy on a periodic basis in line with guidance notes from the Data Protection Commissioner, the recommended date of review stated on the cover page of this policy and industry best practice.

The current version of this policy is Version 1.00.

Internal compliance audits, as authorised and overseen by management, will be considered as part of any internal review on risk and compliance.

It is a requirement that all staff, employees and volunteers comply with any internal audit or investigation relating to any data protection risk assessment, compliance, breach or any other related matter. The results of any assessment, etc. will be recorded and kept on file, in line with any data retention policy.

3.2 External Compliance

The company may be subjected to any enquiry or audit by the Office of the Data Protection Commissioner.

Any enquiry from the Office of the Data Protection Commissioner is to be referred to Deirdre Mackay.

All staff and employees are required to fully cooperate with any audit by the Office of the Data Protection Commissioner; failure to do so may under the circumstances be considered gross misconduct due to the severity of non-cooperation and or possible outcome to the company.

The company may, at the company's discretion, appoint an external auditor to periodically assess and review the company's data protection policy and practices. In such cases, all staff and employees are expected to fully cooperate with any such appointed auditor.

The company may, at the company's discretion, outsource one or more of its role and responsibilities under the Data Protection Acts. The Company recognises that in such a case the company is still considered a data controller under the Data Protection Acts and an appropriate data processing agreement, between the company and data processor, shall be in place.

3.3 Data Protection / Privacy Impact Assessments

A Data Protection Impact Assessment (DPIA), which is also known as a Privacy Impact Assessment (PIA), is a risk assessment tool used to ensure the ongoing at the data protection and privacy rights of all data subjects.

Article 35 of the General Data Protection Regulation (GDPR) introduces the concept of a Data Protection Impact Assessment (DPIA) from May 2018 onwards.

A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them). DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation.

In essence a Data Protection Impact Assessment is required for any new or contemplated data processing activity where the processing is, as per Article 35(1), "*likely to result in a high risk to the rights and freedoms of natural persons*".

However, should the company business change, expand or move into an area that may affect the current data processing arrangements then this issue will need to be reassessed.

Part 4: Information & Data Access Requests & Retention

4.1 Information Request (Section 3 request)

Any person has the right to make an information request under Section 3 of the Data Protection Acts. An information request allows an individual to:

- a) find out whether an organisation has information about that individual,
- b) the description of the information that the organisation has about that individual (categories/types of data), and,
- c) the purposes for which the organisation is holding the information.

The company cannot charge an individual for an information request and must provide the information within 21 days of receipt of the request.

Any information request will be held on file in accordance with the company's data retention policy.

For a person to make an information request under Section 3 of the Data Protection Acts they are to put their request in writing to:

Deirdre Mackay
One in Four CLG
2 Holles Street
Dublin 2. D02FP40

Verbal information requests or requests made by email will not be entertained.

In response to the information request, the company must state that the individual has the right to refer the matter to the Data Protection Commissioner if they are unhappy with the outcome, however, the company would ask that the individual appeal the matter to senior management within the company before contacting the Office of the Data Protection Commissioner as the matter may be easily resolved.

The company must also provide the contact details of the Office of the Data Protection Commissioner; i.e. state in any response "For more information please see the Office of the Data Protection Commissioner's website at www.dataprotection.ie".

Note: An 'information request' under Section 3 of the Data Protection Acts is not the same as an 'information request' under the Freedom of Information Act. One in Four Ireland CLG is not an organisation mandated to supply information under the Freedom of Information Act.

4.2 Access Request (Section 4 request)

Any person has the right to make a data access request, in writing, under Section 4 of the Data Protection Acts for a copy of their personal information held by us.

The company charges €6.35 for a data access request; cheques are to be made payable to “One in Four Ireland CLG”, and the information must be sent to the individual within 40 days of the request.

Due to the sensitive nature of personal data, the company must satisfy itself as to the identity of the individual making the request. The company is entitled to, and best practice demands, that a copy of the individual’s proof of identification accompanies any access request (passport, driver’s licence, etc.) to ensure the individual is entitled to access the data.

Any access request and identification provided will be held on file in accordance with the company’s data retention policy.

For a person to make an access request under Section 4 of the Data Protection Acts they are to put their request in writing to:

Deirdre Mackay
One in Four CLG
2 Holles Street
Dublin 2. D02FP40

Verbal access requests or requests made by email will not be entertained.

One in Four Ireland CLG has 40 days to comply with a data access request subject to the provisions of the Data Protection Acts.

In response to the access request, the company must state that the individual has the right to refer the matter to the Data Protection Commissioner if they are unhappy with the outcome, however, the company would ask that the individual appeal the matter to senior management within the company before contacting the Office of the Data Protection Commissioner as the matter may be easily resolved.

The company must also provide the contact details of the Office of the Data Protection Commissioner; i.e. state in any response “For more information please see the Office of the Data Protection Commissioner’s website at www.dataprotection.ie”.

There are exemptions that the company can rely upon for refusing to provide data (discussed below).

Important: Any response to an access request **must be reviewed** to ensure that no personal data relating to any other individual is included in the response as this would be a breach of the Data Protection Acts. Any response must also be reviewed to ensure that none of the listed exemptions (detailed below) are included in the response.

4.3 Exemptions to providing data in response to an Access Request

Section 5 of the Data Protection Acts set out some exemptions to the right of access. Access to personal data may be refused. These include:

- If the data is subject to legal professional privilege, meaning the data was created following legal advice from a lawyer, and/or the data was created specifically for an upcoming court case.
- Where the requester is involved in a claim against an organisation, seeking compensation and the information reveals details of the organisation's decision process in relation to their claim.
- If the information is held for statistical purposes, is not shared with any other person or organisation and cannot be identified as belonging to any particular individual (i.e. non-personal data).
- If releasing the data would mean that personal data about another individual would be unfairly disclosed. Personal data may be released in redacted form so as to protect the other individual's data.
- Where the data being sought involves personal opinions that have been expressed by another individual. Specifically, if the opinion was given in confidence, and it can be proven that the person providing the opinion at the time did so in the expectation of confidence, it does not have to be released. (If the opinion was given as part of regular business communications, does not involve personal opinions, and was given without the expectation of confidentiality, it should be released).
- If the personal data requested is impossible to supply, or supplying it would be extremely difficult (disproportionate effort).
- If the personal data has already been supplied in accordance with an access request, but identical requests continue to be made (unless new data has been created since the previous records were released, in which case the updated data must be provided).
- If the data that is requested is not the personal data of the requester, it cannot be released under an access request.
- If there is a legal confidentiality imposed due to application of a specific statutory provision e.g. the personal data is considered part of a protected disclosure made in confidence under the Protected Disclosures Act 2014, a mandatory disclosure of a criminal offence under Section 9 of the Criminal Justice Act 2011, etc.
- If the data is stored for back-up purposes, i.e. providing the data would just be providing an additional copy of what was already being sent to the individual.

If there is any doubt as to whether a disclosure relates to any legal proceedings, or potential threat of legal proceedings, **refer the matter to senior management to obtain legal advice.**

4.4 Correcting Data

Following a data access request under Section 4 of the Data Protection Acts an individual may discover that the information held by the company is incorrect, inaccurate or out-of-date.

In such cases, the individual is entitled to have any incorrect personal data corrected, free of charge. They are also entitled to have any out-of-date information deleted or destroyed as soon as possible in accordance with the company's data retention policy.

For an individual to have their data corrected or deleted or destroyed (at their request) they are to put their request in writing to:

Deirdre Mackay
One in Four
2 Holles Street
Dublin 2

Alternatively an individual can email their request to correct data to dmackay@oneinfour.ie

4.5 Data Retention Policy

One in Four Ireland CLG has a personal data retention period of seven years.

This retention period is based upon the general six year limitation period stated in the Statute of Limitations for most causes of action, plus one additional year to allow for service of legal proceedings, equating to seven years in total.

Exceptions to the above limitation period include:

- tax record and payroll records for taxation purposes that are subject to Revenue retention periods;
- Employment interviews and data relating to interview and selection of potential employees (e.g. CVs, cover letters, etc.) of which data relating to unsuccessful candidates will be retained for one year after the closing of the relevant selection period, or job interviewed, to allow service relating to any matter that may arise relating to the selection or employment process (e.g. access to employment under the Employment Equality Acts);
- Data that may assist in the reporting, investigation or litigation relating to a criminal that may reasonably affect the company.
- Any data which management deem appropriate under the circumstances to retain outside the standard seven year retention period, subject to regular reviews as to the necessity of retaining such data that will be destroyed once no longer required.
- Data relating to relevant accidents will be held for ten years:

The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) mandates the company must report and investigate certain accidents in the workplace.

As part of this investigation process, the company must retain certain information relating to an accident, e.g. parties involved, causes, investigation, outcome, CCTV footage (if available) for a period of ten years.

Section 226 of The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) as, inserted by Section 6 of Safety, Health and Welfare at Work (General Application)(Amendment)(No. 3) Regulations 2016 (S.I. No. 370 of 2016), specifically states a mandatory ten year period to retain records relating to a relevant accident.

Part 5: Data Breach Management

5.1 Introduction

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted or unsecure environment. This includes instances in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. Other names for a data breach include an ‘unintentional information disclosure’, a ‘data leak’ or a ‘data spill’.

A data breach may occur for a number of reasons that include:

- Theft or loss of equipment on which data is stored (e.g. memory stick, laptop, etc.)
- Unprotected or easy access to organisational network or software (e.g. no password protection, etc.)
- Human error (e.g. sending an email to the wrong person, etc.)
- Access to information obtained via deception (e.g. ‘social engineering’ where someone pretends to be an authorised person to get information that allows them access secured data).

5.2 Management of a Data Breach in One in Four Ireland CLG

There are three main steps in dealing with a data breach.

1. Incident reporting,
2. Notification of data breach & risk assessment (inc. whether a breach must be notified to the Data Protection Commissioner),
3. Evaluation and Response.

5.2.1 Incident Reporting

Once an employee becomes aware of, or suspects, a data breach they are to report it to their line manager who will escalate it to senior management and or the designated person responsible for all data protection matters. This person is Deirdre Mackay.

In order to investigate properly, the following needs to be included, where possible, in any exculpation of a data breach:

- a) Date and time of the incident;
- b) Date and time the breach was detected;
- c) Description of the incident;
- d) Who reported the incident and to whom;
- e) The type and categories of data involved;
- f) The number of individuals affected by the breach;
- g) Whether the data was encrypted;
- h) Details of any hardware or software involved (e.g. which computers, specific software involved, etc.);
- i) Any corroborating or supporting materials.

5.2.2 Notification of Data Breach & Risk Assessment (Internal)

Internal Notification

A data breach, or suspected data breach, must be reported to a line manager without delay who will in turn notify the organisation's nominated data protection person.

A line manager, in line with the organisation's nominated person, will assess the incident details and risks involved including:

- a) What type and categories of data are involved?
- b) How sensitive is the personal data involved, if any?
- c) What protections were in place to reduce the risk of any breach?
- d) How many data subjects have been affected by the breach?
- e) What are the potential adverse affects for data subjects?
- f) What is the likelihood of damage or loss to data subjects?
- g) What is the potential damage to data subjects?

In circumstances where there is no notification of the Office of the Data Protection Commissioner, the organisation 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. This record should include a brief description of the nature of the incident and an explanation of why the organisation 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.

5.2.3 Notification of Data Breach & Risk Assessment (External)

External Notification

The Office of the Data Protection Commissioner has issued guidelines to what is considered a 'mandatory breach notification' which are dealt with under the following section (see *Notifiable Breach*).

If a breach is considered a notifiable breach, then nominated data protection person will seek appropriate legal advice and also notify the Office of the Data Protection Commissioner via telephone, fax or email at info@dataprotection.ie within **two working days** of becoming aware of the incident.

If notifying the Office of the Data Protection Commissioner of a data breach **do not** include a copy or copies of the data that was breached as it is not required and may cause a further breach (as you did not have permission to share it).

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.

All affected data subjects are to be contacted by One in Four Ireland CLG and informed of,

- a) a brief outline of the data breach,
- b) the personal data, types and categories of data concerning the data subject that was subject to the breach,
- c) suggested steps that the data subject might take to ensure the safety of the data subject (e.g. change passwords, etc.),
- d) the fact the organisation has notified the Office of the Data Protection Commissioner of the breach, and,
- e) any steps taken by the organisation to rectify the situation.

If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access then there may be 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. However, best practice may be to inform data subjects regardless as if the data were to subsequently become accessible then it may cause additional difficulties for data subjects.

In circumstances where a breach has been due to, in part or in whole, deception, hacking, fraud, threats or damage to company property, then the matter may be referred to An Garda Síochána.

In some circumstances, where the health, safety and wellbeing of a person is at risk from a breach then notification to the Health Services Executive may be warranted.

5.2.4 What Constitutes a ‘Notifiable Breach’?

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.

The only exception is where the incident has been:

a) Reported without delay to all the affected data subjects

and

b) It affects no more than 100 data subjects

and

c) It does not include sensitive personal data or personal data of a financial nature.

In other words, if the breach affects over 100 individuals and included sensitive personal data or an individual’s financial data then you must report it to the Office of the Data Protection Commissioner.

If the organisation is unsure as to whether a data breach is a ‘notifiable data breach’ then best practice is follow the Data Protection Commissioner’s guide notes and contact the Office of the Data Protection Commissioner for a determination as to whether the breach was a notifiable breach..

5.2.5 Data Protection Commissioner's role following a Notifiable Breach

Following a notifiable breach, should the Office of the Data Protection Commissioner request the organisation 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:

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

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 the organisation has not already done so.

All staff, employees and volunteers of One in Four Ireland CLG are required to fully cooperate in any investigation by the Office of the Data Protection Commissioner.

5.2.6 Evaluation Response

Following any data breach or any notification, enquiry or investigation from the Office of the Data Protection Commissioner a thorough review of the incident will be made by the organisation with oversight from senior management.

The purpose of this review is to:

- a) ensure that any or all steps taken during the incident were appropriate under the circumstances;
- b) describe and record any and all measures being taken to prevent repetition of the incident;
- c) identify any areas that can be improved and make recommendations of same;
- d) document any recommended changes to policy and or procedures; and,
- e) implement any recommended changes to policy and or procedures as soon as possible.

Part 6: Awareness Training & Support for Staff

6.1 Introduction

One in Four Ireland CLG endeavours to support all staff and employees who process personal data through Data Protection Awareness Training and Data Protection Support.

6.2 Data Protection Awareness Training

Data Protection Awareness Training will take place during induction of new staff and at various periodic intervals through an employee's professional career with One in Four Ireland CLG. Training will also be provided at any important change or development in data protection legislation or best practices as the case may be.

As part of any Data Protection Awareness Training, a familiarity and understanding of this Data Protection Policy is required.

Any updates in legislation and best practices will be incorporated into the next review of this Data Protection Policy. Any relevant guidance notes or press releases from the Data Protection Commissioner or Office of the Data Protection Commissioner are to be inserted into **Annex 3** and to be incorporated into the next policy review.

Staff are required to keep abreast of **Annex 3** which is incorporated into this policy.

6.3 Data Protection Support

Data protection support is provided by Deirdre Mackay who will be able to assist any staff, employees and volunteers with any question or query they may have in relating to data protection.

Conclusion

This Data Protection Policy shall be reviewed at regular periodic intervals to ensure that it complies with current data protection legislation and best practice. It shall also be reviewed to ensure it remains comprehensive and easy to understand.

The next date of review for this document is November 2018.

The document may be reviewed earlier should any new data protection legislation come into effect in the meantime.

Annex 1: Health & Safety matters

Health and safety of employees straddles employment legislation, health and safety legislation and the Data Protection Acts.

Accidents/Injuries

The Safety, Health and Welfare at Work (Reporting of Accidents and Dangerous Occurrences) Regulations 2016 mandates that employers must report certain accidents and dangerous occurrences to the Health and Safety Authority. The full reporting conditions are beyond the remit of this Data Protection Policy.

In order to report, an employer may be required to share some personal data of those involved and/or high level medical data in order to report the severity of any accident or injury, usually after some form of investigation. In such cases, this Data Protection Policy applies to all steps involved in complying with all Health & Safety requirements, e.g. from the initial investigation and reporting stage right through to the final outcome and storage/filing of the report.

Data retention relating to certain accidents

The company identifies that data relating to certain accidents is excluded from the company's general data retention policy of seven years.

Section 226 of The Safety, Health and Welfare at Work (General Application) Regulations 2007 (S.I. No. 299 of 2007) as, inserted by Section 6 of Safety, Health and Welfare at Work (General Application)(Amendment)(No. 3) Regulations 2016 (S.I. No. 370 of 2016), specifically states a mandatory ten year period to retain records relating to a relevant accident.

All records, including personal data, relating to a relevant accident is subject to a mandatory ten year retention period under the above regulations. At the end of the mandatory retention period all records will be destroyed except in the event on any ongoing legal action that necessitates their ongoing retention.

Sick Leave/Medical Certificates

As per an employee's contract of employment and employee handbook, employees are required to certify short-term medical absences from work or short-term sick leave' via a 'high level' report or note from a qualified doctor. The purpose of such a 'high level' report or note is to identify whether in the opinion of a medical expert that an employee was unfit for work for specific dates and also identifies when, in that expert's opinion, an employee is fit for work (at the expiration of the 'sick leave').

The processing of any medical reports or sick leave reports will be conducted in accordance with the Data Protection Policy. As such, any relevant medical notes or reports are stored in a secured physical location with limited access and are destroyed once no longer necessary.

Annex 2: Updates

Relevant guidance notes and press releases from the Data Protection Commissioner and Office of the Data Protection Commissioner

Any guidance notes and or press releases are to be inserted into this annex so as to enable the organisation to keep up to date of current data protection matters.

Any materials inserted into this annex will be reviewed at the next review date of the data protection policy to in order to incorporate them into the next version of the data protection policy.