County Roscommon Disability Support Group CLG

Data Protection Policy and Procedure

Title of Policy and Procedure:	Data Protection	**Document Developed By:**	Development Committee
Policy Area:	Records	**Document Approved By:**	Board of Directors
Responsibility for Review and Audit:	Management and Development Committee	**Responsibility for Implementation:**	Management

	Name	**Title**	**Date**
Author:	Margaret Bourke	CEO	April 2017
In Conjunction with:	BOM	Development Committee	April 2017
Reviewer(s):	Margaret Bourke	CEO	April 2017
	GL, BC, & MaryG	Management Team	April 2017
Authoriser:	Margaret Bourke	CEO	April 2017
BOM Approval Details:	BOM Team	BOM Team	April 2017

Revision Control Log

Version	Date	Change	BOM Approval Date
002	April 2018	Amend responsible person, add appendices, add GDPR references	16th May 2018
003	Oct 2018	Amend as per Hugh Jones template	28th Nov 2018
004	May 2019	Include reference to FLC & appendix 10.6	N/A – M.B. approved

Table of Contents

1.0 Policy Statement

County Roscommon Disability Support Group CLG (RSG)[1] and RSG Flexible Learning College, both entities here in referred to as RSG, is a data controller under the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 and therefore must adhere to the 8 data protection principles. This policy and procedure is in place to ensure compliance with data protection law.

RSG needs to collect personal information to effectively carry out everyday business functions. Such data is collected from employees, suppliers and clients/service users. Such information includes but is not limited to, name, address, email address, date of birth, identification numbers, private and confidential information, Board of Management Minutes and other relevant sensitive information.

In addition, RSG may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however RSG are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), Irish data protection laws and any other relevant the data protection laws and codes of conduct (herein collectively referred to as "the data protection laws").

RSG has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities.

2.0 Purpose

The purpose of this policy is to outline employees, service users, volunteers and employers' rights and responsibilities under the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. RSG is committed to complying with its legal obligations with regard to the Acts.

It is also the purpose of this policy is to ensure that RSG meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and in the individual's best interest.

The data protection laws include provisions that promote accountability and governance and as such RSG has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

[1] Herein after referred to as RSG.

3.0 Scope

This policy applies to all staff within RSG (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in Ireland or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4.0 Legislation and Related Policies

4.1 Legislation

- Data Protection Act 2018
- Data Protection Act 1988
- Data Protection (Amendment) Act 2003
- S.I. 82 of 1989 (Health data)
- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
- Data Protection EU Directive 95/46/EC
- The General Data Protection Regulation (GDPR) (May 2018)

4.2 Related Policies and Procedures

- CCTV Policy
- Consent Policy
- HR and Recruitment Policy and Procedure
- Interview Policy
- Gardaí Vetting Policy
- Employee Handbook

5.0 Glossary of Terms and Definitions

5.1 Organisation

Refers to County Roscommon Disability Support Group CLG.

5.2 Policy

A policy is a written statement that clearly indicates the position and values of the organisation on a given subject (HIQA 2006).

5.3 Procedure

A procedure is a written set of instructions that describe the approved and recommended steps for a particular act or sequence of events.

5.4 Scope

This includes both the target users and target population (only refer to a target population if the policy and procedure is referring to specific groups) of the policy and procedure. It identifies to whom the policy and procedures applies.

5.5 Definitions

5.5.1 **"Data"** means information in a form which can be processed. It includes both automated data and manual data.

5.5.2 **"Data Controller"** are those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as G.P.s, pharmacists or sole traders.

5.5.3 **"Biometric Data"** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

5.5.4 **"Binding Corporate Rules"** means personal data protection policies which are adhered to by the Company for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.

5.5.5 **"Consent"** of the data subject means 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.

5.5.6 **"Cross Border Processing"** means processing of personal data which:

- takes place in more than one Member State; or
- which substantially affects or is likely to affect data subjects in more than one Member State
- in this instance the "**Data controller**" means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

5.5.7 **"Data Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

5.5.8 **"Data Protection Laws"** means for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws that the Company complies with.

5.5.9 **"Data Subject"** means an individual who is the subject of personal data.

5.5.10 **"GDPR"** means the General Data Protection Regulation (EU) (2016/679).

5.5.11 **"Genetic Data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

5.5.12 **"Personal Data"** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5.5.13 **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5.5.14 **"Profiling"** means 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, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

5.5.15 **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

5.5.16 **"Supervisory Authority"** means an independent public authority which is established by a Member State.

5.5.17 **"Third Party"** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority.

6.0 Roles and Responsibilities

The IT Officer is the Data Protection Liaison for RSG.

The Board of Management has overall responsibility for ensuring compliance with data protection legislation.

All Board of Management Members and Employees must co-operate with the Data Protection Liaison when carrying out his/her duties.

The Data Protection Liaison is also available to answer queries or deal with Employees, service users and volunteers' concerns about data protection.

6.1 Objectives

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Company ensures that:

6.1.1 We protect the rights of individuals with regards to the processing of personal information.

6.1.2 We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws.

6.1.3 Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles.

6.1.4 Personal data is only processed where we have verified and met the lawfulness of processing requirements.

6.1.5 We only process special category data in accordance with the GDPR requirements.

6.1.6 We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.

6.1.7 All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and the Company.

6.1.8 Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws.

6.1.9 We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary.

6.1.10 We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements.

6.1.11 We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection – please refer to Appendix 10.2 Data Protection Personal Data Security Breach Report Form.

6.1.12 We have appointed a [Data Protection Officer/Responsible Person] who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR.

6.1.13 We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance.

6.1.14 We provide clear reporting lines and supervision with regards to data protection.

6.1.15 We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes.

6.1.16 Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6.1.17 Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice.

6.1.18 Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements.

6.1.19 We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place.

6.2 Governance Procedures: Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by the Company, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main governance objectives are to:

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance.
- Provide a dedicated and effective data protection training program for all employees.
- Identify key stakeholders to support the data protection compliance program.
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role.
- Identify, create and disseminate the reporting lines within the data protection governance structure.

The technical and organisational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

6.3 The Data Protection Officer (*Data Protection Liaison in RSG*)

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where:

- The processing is carried out by a public authority or body (*except for courts acting in their judicial capacity).*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Where the Company has appointed a designated [DPO/Approved Person], we have done so in accordance with the GDPR requirements and have

ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the Company in monitoring our internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements.

7.0 Procedure

The General Data Protection Regulation (GDPR) (EU) 2016/679) was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a 'Regulation' rather than a 'Directive', its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation. The GDPR came into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive. Under the Data Protection Acts and GDPR, employees, service users, volunteers of RSG have a right to obtain a copy of any information relating to them kept on a computer or in a structured manual filing system regardless of when the data was created.

Personnel records held by Employers come within the terms of the Acts.

Service user's personal and personal health information come within the terms of the Acts and volunteer personal information come within the terms of the Acts.

Employees can make access requests for information held about them – please refer to Appendix 10.3 Data Protection Data Subject Access Request (SARS) Form.

As RSG processes personal information regarding individuals (data subjects), RSG are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

RSG aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights. Please refer to Appendix 10.4 Employee Data Privacy Notice and Appendix 10.5 Service User Data Privacy Notice.

RSG's Flexible Learning College processes the personal data of learners, tutors and other stakeholders with whom it comes into contact. The purposes for which the College processes personal data include:

- The organisation;
- Administration and assessment of programmes of study;
- The provision of supports to learners;
- Promoting our programmes of study;
- The recruitment and management;
- Event and accommodation provision and management;
- Compliance with statutory, contractual and regulatory obligations;

- Compliance with the conditions of funding schemes;
- The safety and security of the College premises.

Please refer to Appendix 10.6 Flexible Learning College Learner Data Privacy Notice.

7.1 Personal Data

Information protected under the GDPR is known as "personal data" and is defined as:

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

RSG ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** (*previously sensitive personal data*), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that:

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

7.2 Data Protection Principles

RSG has the responsibility to protection all personal and sensitive data concerning staff and service users. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Both staff and service users have the right of access to data which has been collected concerning them, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority. GDPR is designed to give individuals more control over their personal data.

Under the Data Protection Acts and GDPR, data must be:

7.2.1 Obtained and processed fairly.

7.2.2 Accurate, complete and kept up to date.

7.2.3 Obtained only for one or more specified, explicit and legitimate purpose.

7.2.4 Shall not be processed in a manner incompatible with these purposes.

7.2.5 Adequate, relevant and not excessive.

7.2.6 Shall not be kept longer than is necessary.

7.2.7 Should be controlled with appropriate security measures.

7.2.8 Give a copy of his/her personal data to an individual on request.

7.2.9 The key principles under the GDPR are:

7.2.9.1 Lawfulness, fairness and transparency;

7.2.9.2 Purpose Limitation;

7.2.9.3 Data minimisation;

7.2.9.4 Accuracy;

7.2.9.5 Storage Limitation;

7.2.9.6 Integrity and confidentiality and - Accountability.

7.3 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be:

7.3.1 Processed lawfully, fairly and in a transparent manner in relation to the data subject (***'lawfulness, fairness and transparency'***).

7.3.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (***'purpose limitation'***).

7.3.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (***'data minimisation'***).

7.3.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (***'accuracy'***).

7.3.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (***'storage limitation'***).

7.3.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (***'integrity and confidentiality'***).

7.3.7 Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' (***'accountability'***) and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

7.4 The Office of The Data Protection Commissioner (DPC)

The DPC is an independent regulatory office whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes:

- The Data Protection Acts 1988 and 2003 (pre-25th May 2018).
- General Data Protection Regulation (post-25th May 2018).
- The Privacy and Electronic Communication (EU Directive) Regulations 2011.

The DPC's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the DPC, as Ireland's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in Ireland.

The Company are registered with the DPC and appear on the Data Protection Register as a [**controller and/or processer***] of personal information.

7.5 Storage of Personal Data

Employee data kept by RSG shall normally be stored **in** the Employee's personnel file / Employee's training file or the Payroll System. Highly sensitive data such as medical reports will be stored in a separate file in order to ensure the highest levels of confidentiality. RSG will ensure that only authorised personnel have access to an Employee's personnel file. It may be necessary to store certain other personal data e.g. salary details will be stored on the payroll system. The Employee's Manager or Supervisor may have access to certain personal data where necessary. Office Staff have access to certain Employee Details.

Service User data is kept in individual files and retained by the service co-ordination team.

Volunteer information is kept **in** individual files and retained by volunteer co-ordinator.

RSG has appropriate security measures in place to protect against unauthorised access.

7.6 Collection and Storage of Data

RSG processes certain data relevant to the nature of the Employment.

RSG will ensure that personal data will be processed in accordance with the principles of data protection, as described in the Data Protection Acts, 1988 and 2003.

Personal data is normally obtained directly from the Employee concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties e.g. references from previous Employers.

Service user information including personal health information is normally obtained directly from the service user and/or their representative, health care professionals and the HSE.

Volunteer personal information is obtained directly from the volunteer.

7.7 Changes In Personal Details

Employees are responsible for ensuring that they inform the HR and Training Manager of any changes in their personal details e.g. change of address. RSG will endeavour to ensure personal data held is up to date and accurate.

Service users or representatives are responsible for ensuring that they inform the Services co-ordination team of any change in their personal details e.g. change of address.

Volunteers are responsible for ensuring that they inform the Volunteer Co-ordinator of any changes in their personal details.

RSG is under a legal obligation to keep certain data for a specified period of time.

In addition the organisation will need to keep personnel data for a period of time in order to protect its legitimate interests.

Accordingly, the personal health information of each service user will be maintained and retained in compliance with Data Protection law. Service user's information will be maintained for a period of ten years. At the end of this period, records will be securely destroyed.

7.8 Security and Disclosure of Data

RSG shall take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data.

Security measures will be reviewed from time-to-time having regard to the technology available, the cost and the risk of unauthorised access. Employees must implement all company security policies and procedures e.g. use of computer passwords, locking filing cabinets etc.

HR data will only be processed for Employment-related purposes and in general will not be disclosed to third parties, except where required or authorised by law or with the agreement of the Employee. HR files are normally stored in the office of the HR & Training Manager and Employees who have access to these files must ensure that they treat them confidentially.

Personal and personal health information of service users will only be processed for the purpose of informing care, treatment or service provisions and should not be disclosed to a third party unless the service user has consented.

Service user files are normally stored in the Services Co-ordination team's office and employees who have access to these files must ensure that they treat them confidentially.

Electronic data is security by means of encryption which is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network. All staff are encouraged to use the automatic lock activation and/or manual locking of their workstation every time he/she leaves the computer unattended.

In the event of RSG ceasing to provide services, informed consent of the service user is required for the transfer of personal information and personal health information to another Service Provider and/or HSE.

In relation service users' home care plans, plans must be maintained at the service users' home and must be made available to the relevant Home Care Support Workers, all health care professional involved in the service users' care and to the HSE.

Volunteer's personal information will only be processed for volunteer-related purposes and in general will not be disclosed to third parties, except where required or authorized by law or with the agreement of the volunteer. Volunteer files are normally stored in the office of the Volunteer Co-ordinator. Employees who have access to these files must ensure that they treat them confidentially

Employees must maintain the confidentiality of any data they have access to in the course of their Employment.

Employees must adhere to the data protection principles set out above.

To ensure compliance with the Data Protection policy and procedure all members of the workforce will receive appropriate data protection training in

accordance with their specific need and their level of access to personal and personal health information.

If Employees are in any doubt regarding their obligations they should contact the Data Protection Liaison.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal and reporting of the breach to the Data Protection Commission.

7.9 Employee Medical Data

The Organisation requests that prior to employment Employees visit their Doctor and get written confirmation of their fitness to work. This data will be retained by the Organisation.

Occasionally, it may be necessary to refer Employees to the company doctor for a medical opinion and all Employees are required by their contract of employment to attend in this case. The Organisation will receive a copy of the medical report, which will be stored in a secure manner with the utmost regard for the confidentiality of the document.

Employees are entitled to request access to their medical reports. Should an Employee wish to do so, please contact the HR & Training Manager who will consult with the doctor who examined you and request **your** data.

The final decision lies with the doctor to decide whether the data should be disclosed to you or not in accordance with Statutory Instrument No. 82 of 1989.

Employees are required to submit sick certificates in accordance with the sick pay policy. These will be stored by the Organisation having the utmost regard for their confidentiality.

7.10 Interview Records

The Organisation will retain records of interview notes, application forms etc. in order to ensure compliance with the Employment Equality Acts, 1998 and 2012 and with the Organisation's Equal Opportunities Policy for a period of 12 months.

7.11 Email Monitoring

The Organisation provides email facilities and access to the internet. In order to protect against the dangers associated with email and internet use, screening software is in place to monitor email and web usage. Mailboxes are only opened upon specific authorisation by a Manager in cases where the screening software or a complaint indicates that a particular mailbox may contain material which is dangerous or offensive; where there is a legitimate work reason or in legitimate interest of the company.

Please see the Email and Internet Usage Policy for further details.

7.12 Close Circuit Monitoring

The Organisation has close circuit television cameras located at a number of locations around the DALE Centre and the Resource Centre. Please see CCTV Policy for further information in relation to specific locations of CCTVs. CCTV is necessary in order to protect against theft or pilferage, for the security of staff and company property. Access to the recorded material will be strictly limited to authorised personnel. Close circuit surveillance is not used to manage performance.

7.13 Access Requests

Employees, service users and volunteers are entitled to request data held about them on computer or in relevant filing sets. This includes personnel records held by RSG. The company will provide this data within 40 days of formal request. Employees, service users and volunteers should make a request in writing to the data protection liaison, stating the exact data required.

Persons are only entitled to data about themselves and will not be provided with data relating to others or third parties. It may be possible redact the data relating to a third party or conceal his/her identity, and if this is possible the Organisation may do so.

Data that is classified as the opinion of another person will be provided unless it was given on the understanding that it will be treated confidentially. Employees who express opinions about other employees, services users and volunteers in the course of their employment should bear in mind that their opinion may be disclosed in an access request, e.g. performance appraisals.

An employee or volunteer who is dissatisfied with the outcome of an access request has the option of using the organisation's grievance procedure.

A service user who is dissatisfied with the outcome of an access request has the option of using the organisation's complaints policy and procedure.

7.14 Right to Object

Employees, service users and volunteers have the right to object to data processing which is causing them distress. Where such objection is justified, the Organisation will cease processing the data unless it has a legitimate interest that prevents this. The Organisation will make every effort to alleviate the distress caused to the individual.

An objection should be made in writing to the Data Protection Liaison, outlining the data in question and the harm being caused to the employee, service user or volunteer.

7.15 Contract with External Bodies

When RSG will need to engage the services of a sub-contractor or agent to process personal data on its behalf. Such an agent is termed a 'data processor' under the Data Protection Acts e.g. a payroll company. Therefore, RSG as data controller must ensure that the all data protection standards are maintained. A data controller can do business with a data processor only on the basis of a written contract which includes appropriate security and other data protection safeguards.

The key points for consideration are:

7.15.1 The Data Protection Acts place responsibility for the duty of care owed to personal data on RSG the Data Controller and accordingly when drawing up the contract RSG the Data Controller should be very specific in the instructions given as to what the Contractor/Data Processor can do with the personal data provided. In particular, the contract should specifically provide that the Contractor/Data Processor will process personal data only on the basis of the authorisation and instructions received from the Contractor/Data Processor. This provision ensures that personal data passed on to a data processor may not be retained or used by the Contractor/Data Processor for its own purposes.

7.15.2 The contract must commit the Contractor/Data Processor to apply appropriate security measures to the personal data to protect it from unauthorised access or disclosure. This provision ensures that the standard of security must be maintained when the personal data is passed from the data controller to its agent.

7.15.3 The deletion or return of the data upon termination or ending of the contract.

7.15.4 Any penalties in place should the terms of the contract be broken.

7.15.5 It would also be expected that RSG the Data Controller or their agents would have a right to inspect the premises of the Contractor/Data Processor as to ensure compliance with the provisions of the contract.

7.15.6 If RSG the Data Controller is required to register with the Office of the Data Protection Commissioner, the Contractor/Data Processor must also register with the Office of the Data Protection Commissioner for the duration of the contract.

8.0 Revision and Audit

The monitoring, audit and revision must take place on a consistent, planned ongoing basis, as referenced on the review date on the cover of the policy and procedure. This review and audit date must be agreed by the development committee.

The feedback from the audit must be communicated to the relevant people in order to ensure continuous improvement. This will facilitate the sharing of best practice and learning from experiences and knowledge of what works best in the organisation.

The feedback must also be used to address any barriers to implementation and influence future development of the policy and procedure.

A review will be carried out on a yearly basis unless for example, an audit, serious incident, organisational structural change, scope of practice change, advances in technology, significant changes in international best practice or legislation identifies the need to update the policy and procedure.

9.0 References

9.1 http://www.hiqa.ie/standards/health/safer-better-healthcare (Accessed 27/4/18)

9.2 https://www.hse.ie/eng/services/yourhealthservice/info/dp/data-protection-acts/ (Accessed 27/4/18)

9.3 www.dataprotection.ie (Accessed 27/4/18)

10.0 Appendices

10.1 Data Protection Toolkit: GENERAL DATA PROTECTION LEGISLATION: WHAT CHARITIES NEED TO KNOW - A TOOLKIT FROM DÓCHAS & FP LOGUE SOLICITORS

10.2 Data Protection Personal Data Security Breach Report Form

10.3 Data Protection Data Subject Access Request (SARS) Form

10.4 Employee Data Privacy Notice

10.5 Service User Data Privacy Notice

10.6 Flexible Learning College Learner Privacy Notice

10.7 Website Privacy Policy