SCCUL Enterprises CLG | *Of the Community For the Community*

Data Protection Policy

SCCUL Enterprises CLG is a registered charity set up by, but independent to, St. Columba's Credit Union, Galway, in 2002. As a not for profit, social enterprise, SCCUL aims to champion societal change by promoting community, enterprise, wellbeing and social inclusion. This is achieved through a number of successful initiatives operating from the West of Ireland;

1. SCCUL Enterprise Centre, Ballybane
2. bizmentors®
3. Bizmentors International
4. SCCUL Sanctuary, Clarinbridge
5. Ballinfoile Castlegar Neighbourhood Centre

Our **Vision** is: To alleviate poverty and disadvantage by empowering positive well-being and growth.

Our **Mission** is: To facilitate individual, community and economic growth in a sustainable manner, through socio economic development with the provision of supports and infrastructure.

CONTENTS **PAGE**

1. Introduction

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing, storage and security of their personal data. It is the policy of SCCUL Enterprises CLG to comply with the obligations of the Data Protection Acts 1988 and 2003 and to ensure that all employees are aware of their data protection responsibilities.

Employees and service users supply this company with personal information, and Data Protection legislation applies to this information. Data Protection law places obligations on the organisation and all employees who keep personal information. Every individual has the right to know what personal information is held about her/him. The Act applies to living persons.

Data Protection rights apply whether the information is held in paper-based form, in electronic format, in manuals, or in photographs, video or digital images.

Manual files created before July 2003 are not subject to the full application of the Acts until October 24, 2007. However, those files are subject to access on request and security rulings apply to them.

Data Protection Rules

The key responsibilities for the organisation with respect to personal information are as follows:

1. Data should be obtained and processed fairly
2. Data should be kept only for one or more specified and lawful purposes
3. Data should be processed only in ways compatible with the purposes for which it was given to the organisation originally
4. Data should be kept safe and secure
5. Data should be kept accurate and up to date
6. Data should be adequate, relevant and not excessive for the purpose(s) for which it is collected and processed
7. Data should not be retained for any longer than is necessary for the specified purpose(s)
8. An individual will be given a copy of his/her personal data on request

2. Policy Statement

With regards to its data protection responsibilities this company will endeavour to:

- Comply with both the Data Protection Acts and good practice;
- Protect the privacy rights of service users and employees in accordance with Data Protection Acts;

- Ensure that personal information in the organisation's possession is kept safe and secure;
- Support employees to meet their legal responsibilities as set out under data protection rules;
- Respect individuals' rights;
- Provide awareness training and support for employees that process personal information.
-

3. Policy Purposes

The purposes of this Data Protection Policy are:

- To outline how this company endeavours to comply with the Data Protection Acts;
- To provide guidelines for employees;
- To protect this from the consequences of a breach of its responsibilities.

4. Policy Scope

This Data Protection Policy applies to all employees who handle personal data of service users, the people we support and/or employees.

5. Data Protection Principles

This company will endeavour to meet its obligations under the Data Protection Acts and apply the eight Data Protection Principles in how it stores and processes personal data and information.

5.1 Obtain and Process Data Fairly

At the time the personal data is being collected, an individual must be made aware of the following:

- What information is being collected and why it is being collected
- Who within this company will have access to the information
- How the information will be used and What third party disclosures are contemplated
- The consequences of not providing the information (if any)
- Any statutory obligation that may arise to collect the information
- The person's right to access the information, once collected, and the identity of the organisation collecting the information.

The individual must have given consent to the processing of the data. Processing means performing any operation or set of operations on data, including:

obtaining, recording or keeping data, collecting, organizing, storing, altering or adapting the data; retrieving, consulting or using the data; disclosing the data by transmitting,

disseminating or otherwise making it available; aligning, combining, blocking, erasing, or destroying the data.

However, there may be some situations where processing of data may be necessary without the explicit consent of the individual having been obtained:

- compliance with a legal obligation;
- protecting the vital interests of the person where the seeking of the consent of the person is likely to result in those interests being damaged;
- preventing injury to, or damage to the health, of another person; and
- for obtaining legal advice, or in connection with legal proceedings, or is necessary for purposes of establishing, exercising, or defending legal rights.

5.2 Purpose(s) for which information is stored

This principle requires employees processing personal data to be aware:

- That an individual should know the specific reason/s why information is being collected and retained;

- That the purpose for which the information is being collected is a lawful one;

- Of the different categories of data which are held and the specific purpose for each.

5.3 Processing of Data

Data should be processed only in ways compatible with the purposes for which it was given to the organisation originally.

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

- Employees are not to disclose any personal information to any third party without the consent of the individual to whom it refers;

- 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.

5.4 Data should be kept safe and secure

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

- Access to information is restricted to authorised employees on a “need-to-know” basis.

- Computer systems must be password protected.
- Information held on computers must always be protected by a password to prevent unauthorised access.
- There must be back-up procedures in operation for computer-held data.
- Personal information on computer screens should only be visible to the computer user who must have the authority to access the information.
- Employees must be aware of the organisation's confidentiality and security policies and procedures and comply with them.
- Data must be securely disposed of when no longer required, or when the purpose for which the information was obtained is no longer current, relevant or valid.
- Premises must be secure when unoccupied, and personal information should be securely locked away when not in use.

5.5 Data should be kept accurate and up to date

Personal information must be accurate. It is the responsibility of all employees who obtain or hold information to ensure that it is accurate and complete.

Where an individual data subject informs or advises this company of any errors or changes to their data, employees must amend the information accordingly, and as soon as is reasonably possible.

Manual and computer procedures must be adequate to ensure high levels of data accuracy and maintenance.

5.6 Data should be adequate, relevant and not excessive for the purpose(s) for which it is collected and processed

Only the information necessary to provide support or services should be collected and maintained.

Periodic reviews should take place of any personal information already held, to ensure that it is adequate, relevant and not excessive for the purpose for which it was collected.

5.7 Data should not be retained for longer than is necessary for the specified purpose(s)

Data should be held for the length of time the purpose for which it was collected is valid. Once this data is no longer current or valid, it must be disposed of in a secure manner. Particular care is to be taken when shredding or incinerating paper-based or manual data and when disposing of laptops and computers.

Exceptions may apply from specific legislation which require information to be retained for particular periods.

5.8 An individual will be given a copy of his/her personal data on request

An individual about whom personal data is held is entitled to:

- A copy of the data held about him/her
- Know the purpose for processing his/her data
- Know the identity of those to whom the data may be disclosed
- Know the source of the data, unless it is contrary to public interest
- Know the logic involved in automated decisions, and
- Have a copy of any data held in the form of opinions, except where such opinions were given in confidence.
- Know the reasons for an access refusal.

To make an access request the Data Subject must:

- Apply in writing (which may be via email);
- Give any details which might be needed to help identify the individual and locate the information kept about him/her.

In response to a request for access to information this company must:

- Supply the information to the requester promptly and within forty days of receiving the request, and
- Provide the information in a form which will be clear to the person.

Right of access can be refused if:

- Providing access will pose a serious threat to the life or health of any individual, including the requester,
- Providing access would have an unacceptable impact on the privacy of other individuals, or
- It is required or authorised by law.

Additional rights under the Data Protection Acts:

- Data subjects have the right to have any inaccurate information rectified or erased;
- Data subjects have the right to have personal data taken off a mailing list;
- Data subjects gave the right to complain to the Data Protection Commissioner.

6. Procedure for dealing with a request under the Data Protection Acts

Upon receiving a data protection request, the following steps will be taken:

- Data protection request is forwarded to this company designated Freedom of Information Officer.
- The Freedom of Information Officer will check that the access request can be granted under the Data Protection Acts of 1998 and 2003.

- If access may not be granted under the Data Protection Acts, the person requesting access will be notified of this fact and informed of their right to seek access under the Freedom of Information Act.
- If access may be permitted under the Data Protection Acts the following actions will be taken:
    - Date stamp the access request
    - Record and place on file any discussions concerning the request
    - Record the date on the file that a decision will be forthcoming (within 30 days)
    - Check that the request comes within the scope of the Acts. It must be received in writing, reference made to the Data Protection Act, contain sufficient information to identify the records required, clearly identifies who is requesting the information. If a third-party requests information their authority to do so must be clearly stated.

- The Freedom of Information Officer will send a letter acknowledging the access request and access fee to the person/third party making the request within 7 days. The letter will state the date when a decision on the access request will be made.
- If upon investigation it transpires that there is insufficient information to identify the records requested, the person/third party making the request will be contacted by the Freedom of Information Officer to inform them that the request will be suspended until clarifications are received. If despite receiving assistance to clarify the request, it is still not possible to identify the records requested, this company can refuse to process the request. All steps taken to process the request will be clearly documented. The person/third party making the request will be informed of the circumstances leading to this decision.
- If the authenticity of the request is confirmed, the Freedom of Information Officer will arrange to obtain the relevant files from staff holding these files within this company. The location and process and effort involved in assembling the files should be clearly documented. Once all records are assembled, they should be numbered, and a copy made of same. The person within this company who will be responsible for deciding upon the release of information will receive the files for review.
- The decision-maker should agree the method of access to the records (if access is other than by copies of documents being issued by registered post) and blank out any details/data which is considered to be non-disclosable under the Data Protection Acts.
- This company reserves the right to restrict access to information under section 5 of the Data Protection Act and The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. no. 82 of 1989).

7. Right of Complaint to the Data Protection Commissioner

Any person may complain to the Data Protection Commissioner about the way in which their data protection request was handled.

8. Management of a Data Breach

Should a data breach occur, the following actions will be taken.

- Details of the data breach incident will be recorded by the line manager/supervisor. Details should include time and date the breach was reported, the circumstances, I.T. systems used, the data involved, the person to whom the breach was reported, time the breach was detected, if the data was encrypted and any corroborating material.
- The line manager/supervisor should inform the Freedom of information Officer and Corporate Services Manager. If required they will hold an emergency meeting to discuss the data breach incident. This meeting is to discuss the incident and risks arising from the incident.
- Best practice requires that the Office of the Data Protection Commissioner be informed. This is the responsibility of the Freedom of Information Officer.
- In consultation with the Office of the Data Protection Commissioner, a decision will be taken whether the circumstances require the persons whose data has been breached to be notified.
- Other third parties such as An Garda Síochána may need to be notified to help minimise the consequences for the persons whose data has been breached.
- Subsequent to the breach a thorough evaluation of the incident will take place. This review will ascertain if the actions taken during the incident were appropriate and determine what steps should be taken to avoid a repeat of such a data breach.

9. Policy Review

This Data Protection Policy will be subject to review every three years or in response to changes made to amendments to the Data Protection Acts.