Data Protection

Standard Operating Procedure

SOP Title:

Standard Operating Procedure for Data Protection

Document reference number	**SIDP1**	**Document developed by**	**Grainne Muldoon**
Revision number	One	Document approved by	Board of directors, StepIn
Approval date	March, 2014	Responsibility for implementation	All StepIn staff (paid and voluntary)
Revision date	This guidance will be reviewed at least every 2 years. A change in relevant legislation, practice, service requirements or a serious incident will prompt an earlier review.	Responsibility for review and audit	Board of directors, StepIn

1. PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to have uniformity and consistency in relation to management and protection of network members' data by StepIn staff, volunteers and board of directors. This SOP will assist StepIn staff, volunteers and board of directors in outlining the procedure to be followed when working with network members' data.

2. SCOPE

All frontline staff — paid and unpaid — of StepIn and all board of directors

3. INTRODUCTORY STATEMENT

Data protection is about network members' fundamental right to privacy. Network members can access and correct data about themselves. StepIn staff, volunteers and the board of directors may keep data about network members. StepIn staff, volunteers and board of directors have to comply with data protection principles. The main Irish law dealing with data protection is the Data Protection Act 1988. The 1988 Act was amended by the Data Protection (Amendment) Act 2003.

4. ROLES AND RESPONSIBILITIES

It is part of StepIn staff and volunteers' roles to protect members' information and data as laid down in the 1988 Data Protection Act as amended by the Data Protection Amendment Act 2003. This Act must be followed at all times by all staff and volunteers as well as board of directors. It is StepIn's responsibility to ensure that volunteers and staff have the resources available to enable them to follow the Data Protection Act, 1998 effectively. All staff, volunteers and board of directors have certain key responsibilities in relation to the information which they keep on computer or in a structured manual file about network members. These are summarised in terms of eight "rules" which staff, volunteers and board of directors must follow, and which are listed below:

Staff, Volunteers, and Board of Directors must:

4.1 Obtain and process the information fairly.

- Understand and comply with the law: Every use of Network Members identifiable information must be lawful. The board of directors is

responsible for ensuring StepIn complies with legal requirements regarding data protections and confidentiality.

4.2 Keep it only for one or more specified and lawful purposes:

- Network members' identifiable information should not be used unless it is absolutely necessary; network members' identifiable information items should not be used unless there is no alternative and unless the member has consented to this use.

- Use the minimum necessary network member identifiable information: Where use of network members' identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

4.3 Process it only in ways compatible with the purposes for which it was given initially

4.4 Keep it safe and secure

- Access to the network members' identifiable information should be on a strict need to know basis: Only those individuals who need access to network members' identifiable information should have access to it, and they should only have access to the information items that they need to see.

- Electronic Privacy Regulations: This SOP and these guidelines apply to data protection for phone, e-mail, SMS and internet use. Dialogue at board of director meetings, via Skype or phone conferencing and text messaging will also give due consideration to data protection principles. Emails and faxes between board members and staff members and volunteers will also give consideration to their responsibilities regarding data protection.

4.5 Keep it accurate and up-to-date

4.6 Ensure that it is adequate, relevant and not excessive.

- Justify the purpose: Every proposed use or transfer of network members' identifiable information within or from StepIn should be clearly defined and scrutinised, with continuing uses regularly reviewed by staff and volunteers during supervision and at board of director meetings.

4.7 Retain it no longer than is necessary for the specified purpose or purposes.

- Everyone to be aware of their responsibilities: Actions should be taken to ensure that those handling network members' identifiable information (both paid and unpaid staff and board members) are aware of their responsibilities and obligations to respect members' confidentiality. This is done throughout this and various other StepIn standard operation procedure and through regular staff supervision and discussions at board of director meetings and via other forms of communications, e.g. emails, phone consultations etc.

4.8 Give a copy of his/her personal data to any individual, on request.

5. StepIn IT data security protocol

The following points outline practical management of data storage for StepIn staff, volunteers and board members when considering use of network members' information and data within or outside of StepIn.

5.1 Secure, central file management: StepIn stores data information centrally on Google Drive. Google is of good-standing with solid security policies. Data requires an encrypted connection before it can be uploaded — indicated by a padlock beside the url in the browser. Data is stored on Google Drive with no encryption.

5.2. System administration: StepIn uses its administrator to manage IT data

storage. This super-user manages access levels and storage of information.

5.3. Access privileges: Access is allowed according to the roles and responsibilities outlined above.

5.4 Read-only: To ensure constancy of information, StepIn categorises information as read-only or editable documents. Read-only documents may not be altered or edited.

5.5 Private access: The administrator uses only his personal computer to transfer documents to Google Drive. There is no use of computers accessible by others, such as internet cafes.

5.6 Back-up: StepIn data is backed up on a BIPRA 1TB external portable hard drive. The administrator is the only person with access to this storage.

5.7 Dropbox: The board of directors use Dropbox cloud storage for sharing group work that is being progressed by more than one director. Sensitive information, such as network member data, is not shared in this forum. Dropbox is of good-standing with solid security policies: files are stored using 256-bit AES encryption and SSL creates a secure tunnel for data transfers.

6.0 Appendices

6.1 Appendix 1: Data Protection Act 1998 [available at www.dataprotection.ie]

Data Protection Policy signed and dated

Signed: _____

StepIn Chairperson

Date: _____