Sligo Volunteer Centre

Data Protection
Policy and Procedures

Doc. No.	7	**Version No.**	2
Last Reviewed	August 2020	**Approved By**	BOM
Next Review	August 2023	**Responsibility**	CH

Table of Contents

1. Policy

1.1 Policy Statement	Sligo Volunteer Centre is committed to the protection of the rights and privacy of individuals and organisations, including staff, volunteers, Volunteer Involving Organisations (VIOs) and others whose data is held by the organisation. This commitment is underpinned by full compliance with the statutory measures that ensure these rights, namely the Data Protection Act 1988, the Data Protection (Amendment) Act 2003 and the General Data Protection Regulation 2016. To meet our responsibilities under the legislation and in accordance with the data protection principles, we will: 1. Obtain and process information fairly. 2. Keep it only for one or more specified, explicit and lawful purposes. 3. Use and disclose data only in ways compatible with these purposes. 4. Take appropriate measures to keep data safe and secure. 5. Keep it accurate, complete and up-to-date. 6. Ensure it is adequate, relevant and not excessive. 7. Retain for no longer than is necessary for the purpose or purposes it was collected. 8. Provide data to data subjects on request.
1.2 Purpose	1. To outline the rules on data protection and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal data. 2. To provide good practice guidelines for staff and associated stakeholders. 3. To protect Sligo Volunteer Centre from the consequences of a breach of its responsibilities.
1.3 Scope	All staff, volunteers, contractors and representatives handling data for or on behalf of the organisation who have access to data in all formats i.e. paper, electronic or audio-visual.
1.4 Responsibilities	**Board** ● Ensuring resources are in place to meet the requirements of this policy. ● Ensuring the policy and procedures are adequate, up-to-date, in line with legislative requirements and systematically reviewed. ● Designating a Data Protection Officer (DPO). ● Ensuring the DPO has the autonomy and resources necessary to carry out their role effectively and efficient. **Manager** ● Assisting the Board to develop, review and approve the policy and procedures. ● Ensuring the organisation is fully compliant with legislation in its day to day activities. ● Ensuring only authorised personnel engage in activities associated with providing the service. ● Monitoring the implementation of this policy and associated procedures. ● Dealing with concerns arising out of the implementation of this policy.

	Staff ● Complying with the requirements of the policy and associated procedures. ● Creating and maintaining full and accurate records of all activities. ● Handling data with care and respect so as not to compromise their integrity. ● Preventing unauthorised access. ● Bring any observations or concerns to the attention of the manager that may require updates to the policy and procedures. **Data Protection Coordinator** ● Monitor compliance with the General Data Protection Regulation. ● Collect information to identify processing activities. ● Analyse and check the compliance of processing activities. ● Inform, advice and issue recommendations. ● Provide support, assistance and training.

2. Procedures

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH
Procedure Title	7.1 Obtaining and Processing Data		
Purpose	To ensure that all data is obtained and processed in a transparent and effective manner.		
Staff Involved	All Staff		
Procedure	1. Sligo Volunteer Centre and Volunteer Ireland are considered Joint Data Controllers in respect of the Data collected on IVOL, the national database for volunteering. The agreement between the two organisations is in Appendix 1 of this policy. 2. Information may only be collected for the provision of volunteer associated activities which include the following: a) Gather statistics on the age, gender and nationality of volunteers. b) Provide a volunteer placement service. c) Provide a Garda Vetting Service. d) Provide services including, but not limited to, training and consultancy and volunteer programme management. e) Undertake marketing, promotion, direct recruitment and public relations exercises. (Related to volunteering). f) Carry out research into voluntary activities. g) Provide personnel, payroll and pension administration services. h) Update databases. i) Provide online services. 3. The data subject must be made aware of the following prior to processing their data: 1) Reason for collecting the data. 2) How it will be used. 3) Legal basis for processing the data (consent/explicit Consent). 4) Disclosure to third parties. 5) Retention period. 6) Contact details for the DPO. 7) Their rights: - Right to be informed. - Right of access. - Right to rectification. - Right to erasure. - Right to restrict processing. - Right to data portability. - Right to object. - Rights around automated decision making and profiling. - Right to withdraw consent at any time. - Right to make a complaint.		

	4. Personal data should only be processed for the specific purpose(s) notified to the data subject(s) and for which it was gathered in the first place. a) If it is requested to be used for any other purpose consent must be obtained from the data subject(s). (Any requests are subject to board/steering committee approval). 5. Data should only be disclosed for the original purpose it was obtained. 6. Data should not be disclosed to third parties without the consent/explicit consent of the data subject. a) Verbal consent may be obtained for the disclosure of non-sensitive data b) Written consent must be obtained for the disclosure of sensitive data. 7. Sensitive personal data may be disclosed without the express written consent of the data subject in the following circumstances: a) Where the data subject has already been made aware of the person/organisation to whom the data may be disclosed. b) Where it is required by law. c) Where it is required for legal advice or legal proceedings, and the person making the disclosure is a party or a witness. d) Where it is required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State. e) Where it is required urgently to prevent injury or damage to health, or serious loss of or damage to property. 8. Personal information should not be disclosed to work colleagues unless they have a legitimate interest in the data to fulfil official employment duties. 9. Personal data may be used for research purposes under the following conditions: a) Consent of the data subject. b) Personal data must be kept anonymous. 10. Any concerns or queries relating to the obtaining and processing of data should be brought to the attention of the DPO and/or management.
Records	I-Vol, Personnel Files, Retention Schedule, Disposal Log, Emails, Written Correspondence

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH
Procedure Title	7.2 Data Access Requests		
Purpose	To allow an individual access to their personal data		
Staff Involved	All staff, DPO		
Procedure	Once a data request is received the following applies: 1. Inform the individual that the request must be submitted in writing to the DPO using the organisation's access request form (email a form on request). 2. Once the written request is received the DPO will verify the identity of the individual using reasonable means – e.g. request a copy of recent photo I.D. 3. Once verified the DPO will process the request or assign a person to do it. 4. The DPO will track/record results to ensure compliance. (In the event of a dispute a trail must be available to show compliance) 5. Processing the request should be complete within one month of receiving the request in writing. - This time period can be extended by an additional two months if where requests are complex or numerous. - Inform the individual in writing of the extended time period within the 1 month limit. 6. Send the data to the individual in the agreed time electronically unless the individual requests that it be sent manually.		
Records	Access Request Form, Tracking Log, Emails, Written Correspondence		

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH
Procedure Title	7.3 Requests to Rectify, Erase, Restrict or Objections to Processing		
Purpose	To ensure that individual requests are dealt with in a timely and effective manner.		
Staff Involved	All Staff, DPO		
Procedure	Once a request is received the following applies: 1. Inform the individual that the request must be submitted in writing to the DPO. 2. Once the written request is received the DPO will verify the identity of the individual using reasonable means – e.g. request a copy of recent photo I.D. 3. Once verified the DPO will process the request or assign a person to it. 4. The DPO will track/record results to ensure compliance. (In the event of a dispute a trail must be available to show compliance) 5. Processing the request should be complete within one month of receiving the request in writing. a. This time period can be extended by another two months if where requests are complex or numerous. - Inform the individual in writing of the extended time period within the 1 month limit.		

<table>
<tr><td></td><td colspan="3">6. Notify the individual in the agreed timeframe of the results of their request.</td></tr>
<tr><td>Records</td><td colspan="3">Emails, Written Correspondence</td></tr>
<tr><td>Doc. No.</td><td>7.2</td><td>Version No.</td><td>2</td></tr>
<tr><td>Last Reviewed</td><td>August 2020</td><td>Approved By</td><td>BOM</td></tr>
<tr><td>Next Review</td><td>August 2023</td><td>Responsibility</td><td>CH</td></tr>
<tr><td>Procedure Title</td><td colspan="3">7.4 Data Portability Requests</td></tr>
<tr><td>Purpose</td><td colspan="3">To ensure that individual requests are dealt with in a timely and effective manner.</td></tr>
<tr><td>Staff Involved</td><td colspan="3">Manager, All Staff</td></tr>
<tr><td>Procedure</td><td colspan="3">7.4.1 Handling a Request
Once a data portability request is received the following applies:
1. Inform the individual that the request must be submitted in writing to the manager using the organisation’s data request form detailing all data requested (email a form on request).
2. Once the written request is received the manager will:
- Verify or delegate a person who will verify the identity of the individual using reasonable means – e.g. request a copy of recent photo I.D.
3. Once verified the manager will process the request or delegate someone to process it.
7.4.2 Processing a Request
1. Gather all data requested in whatever format it is in.
2. Save all data in a PDF format.
3. Send the data to the data subject for review and agree it.
4. Once agreed send the data in PDF format to the other controller identified by the data subject and request a receipt.

- Processing the request should be complete within one month of receiving the request in writing.
- This time period can be extended to two months where requests are complex or numerous.
- If the time period is to be extended, inform the individual.
4. The manager will track/record results to ensure compliance.
- In the event of a dispute an audit trail must be available to show compliance.
5. The person responsible must send notify the data subject in the agreed timeframe of the results of their request.</td></tr>
<tr><td>Records</td><td colspan="3">Data Request Form, Tracking Log, Emails, Phone Calls, Written Correspondence.</td></tr>
</table>

Doc. No.	7.5	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH
Procedure Title	7.5 Confidentiality and Security		
Purpose	To ensure that information is managed in a consistent, secure and confidential manner.		
Staff Involved	All Staff		
Procedure	Standards of security include the following: 1. Access to I-Vol is limited to authorised personnel who will have individual passwords for access. 2. Access to IT servers is restricted in a secure location to a limited number of staff. 3. Access to any staff personal data is restricted to authorised personnel for legitimate purposes only. 4. Access to computer systems is password protected with other factors of authentication as appropriate to the sensitivity of the data. - Non-disclosure of personal security passwords to any other individual including other personnel is encouraged. 5. Information on computer screens and manual files to be kept out of sight from callers to our offices. 6. Back-up procedures are managed by Sligo County Council. 7. Computers are protected by anti-virus software. 8. Computers have automatic screen savers should the user fail to log out. 9. Personal manual data is to be held securely in locked cabinets, locked rooms, or rooms with limited access. 10. Staff are provided with data protection information and training relevant to their role.		
Records	Training Records, Computer Audit Trail, Log In Details.		

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH

Procedure Title	7.6 Data Cleansing
Purpose	To ensure accurate, up to date data is available to the organisation and that it is in line with data protection legislation and guidelines.
Staff Involved	All Staff
Procedure	**Note:** Sligo Volunteer Centre and Volunteer Ireland are considered Joint Data Controllers in respect of the Data collected on IVOL, the national database for volunteering. The agreement between the two organisations is in Appendix 1 of this policy. Further specific actions around responsibilities for Data Cleansing exist here. **I-Vol** 1. In order to ensure clean data all fields must be complete at time of initial entry on any systems – refer to the I-Vol manual for instructions. 2. The automated system checks for any fields not complete on an ongoing basis. 3. Quality checks are carried out quarterly on a random selection of: - Volunteer Records - Volunteer Involving Organisation (VIO) Records - Volunteering Opportunities 4. Log any issues identified. 5. Create a clean-up plan with responsibility clearly assigned. 6. Contact all VIOs annually to verify and update information. 7. Maintain the database: - Assign responsibility for systematic cleansing. - Update policies and procedures. - Seek external expertise, if required. - Keep staff informed and upskilled. - Carry out random spot checks. - Discuss issues with relevant staff members. - Ensure consistency of data entry among all staff. **Other Data** **1.** All policies and procedures are reviewed annually, as per the document control matrix. **2.** Staff records are updated annually in line with performance reviews or sooner if required. **3.** Information on the website and/or social media is reviewed and updated weekly. **4.** All data is reviewed annually for relevance and updated or disposed of as required.
Records	Quality Reports, Quality Improvement Plan, Record of Meetings, Document Control Matrix

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH

Procedure Title	7.7 Managing a Data Breach
Purpose	To ensure a standardised management approach is implemented in the event of a data breach.
Staff Involved	Manager, DPO, Chairperson of the Board
Procedure	A data breach may happen for a number of reasons, including: - Loss or theft of equipment on which data is stored. - Inappropriate access controls allowing unauthorised use. - Equipment failure. - Human error e.g. send an email to the wrong address. - Unforeseen circumstances such as a flood or fire. - Computer hacking. - Access where information is obtained by deception. Should a breach occur it is to be managed in the following way: 1. Details of the incident should be recorded, including. - A description of the incident. - The date and time of the incident. - The date and time it was detected. - Who reported the incident and to whom it was reported. - The type of data involved and how sensitive it is. - The number of individuals affected by the breach. - Was the data encrypted? - Details of any Information IT systems involved. - Additional material. 2. Notification of the breach and risk assessment. Internal Notification ● A data breach must be reported without delay the senior manager, who in turn will immediately notify the DPO and chairperson of the board/steering committee with the incident details. ● The DPO will immediately convene a meeting of relevant people to deal with the incident. ● The group will assess the incident details and the risks involved, including: - What type of data is involved? - How sensitive is the data involved? - How many individuals' personal data are affected by the breach? - Were there protections in place e.g. encryption? - What are the potential adverse consequences for individuals and how serious or substantial are they likely to be? - How likely is it that adverse consequences will materialise? External Notification ● If there is a risk to the Data Subject, the breach must be reported to the Data Protection Commission within 72 Hours. ● The DPO will be responsible for contacting the office of the data commissioner. ● The management team in consultation with the office of the data commissioner will decide if it is appropriate to inform the persons whose data has been breached.(every incident will not warrant notification). ● If a breach is thought to be High Risk, e.g. in the case of Sensitive personal data being breached, then the data subjects should be notified as soon as

	possible. In situations with less risk a decision can be made in consultation with the DPC. ● When notifying individuals management will consider the most appropriate medium for doing so. It will bear in mind the security of the medium for notification and the urgency of the situation. ● Specific and clear advice will be given to individuals on the steps they can take to protect themselves and, what the organisation is willing to do to assist them. ● The DPO will be the contact person for further or ongoing information. ● The management team will also consider notifying third parties, such as An Garda Síochána who can assist in reducing the adverse consequences to the data subject(s). ● Other statutory agencies will be informed as required. 3. Evaluation and Response ● Subsequent to any breach a review of the incident will be made by management. The purpose of this review will be to: - Ensure that the steps taken during the incident were appropriate. - Describe and record the measures being taken to prevent a repetition of the incident. - Identify areas that may need to be improved. - Document any recommended changes to policy and/or procedures which are to be implemented as soon as possible thereafter.
Records	Record of Meetings, Emails, Quality Improvement Plan, Log of any breaches

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH
Procedure Title	7.8 Internal Audits		
Purpose	To ascertain if the systems in place are ensuring we are operating in accordance with the data protection acts and regulations and to identify any risks or possible non-compliance.		
Staff Involved	DPO		
Procedure	Internal audits will be carried out annually by the DPO, who will. 1. Complete the audit schedule - The schedule specifies the areas and/or processes to be audited, the audit criteria and scope of the audit. - Areas specified in the schedule are audited against relevant documentation and standards (audit criteria). 2. Internal audits are carried out across selected activities annually, with greater frequency, if required. - The frequency of audits can be adjusted depending on the results of previous audits, feedback, new procedures or the importance of an identified issue. 3. The audits are carried out by: - Reviewing manual and electronic procedures and compliance. - Consultation with relevant staff. - Reviewing previous audit reports and improvement plans. 4. A summary internal audit report is completed by the DPO outlining any strengths and areas for improvement. - Where an issue is discovered it is recorded on the QIP. (Issues will be prioritised for completion) - The issue and corrective action should be agreed between the auditor and the person tasked with completing the corrective action. - Where no issues are found a record is retained to signify that an audit has been carried out, i.e. an audit report must still be completed. 5. Corrective actions are checked at the end of each month by the PO to verify completion. 6. Reports are provided to the next board meeting for review. 7. Internal audit reports are to be maintained for a period of three years.		
Records	Audit reports, Quality Improvement plan, Corrective Action Log, Quality Control Check reports IVOL		

Last Reviewed	August 2020	**Approved By**	BOM
Next Review	August 2023	**Responsibility**	CH
Procedure Title	7.9 Awareness Training and Support		
Purpose	To ensure that staff have the necessary knowledge and skills to carry out their activities giving due care to the data they have access to,		
Staff Involved	Senior Management, DPO, Volunteer Ireland staff (due to Joint Data Controller Agreement in respect of IVOL)		
Procedure	1. Initial data protection information will be provided at induction. 2. All new staff members will receive beginner level I-Vol training provided by the super administrator. 3. The DPO will provide periodic updates and awareness training as required. 4. I-Vol upskilling workshops will be held annually. 5. I-Vol manual will be reviewed and updated annually or sooner if required. 6. Updates will be communicated to stakeholders electronically. 7. A tricks and tips forum will be available to users on an ongoing basis. 8. Salesforce regional champions will provide ongoing advice and support.		
Records	Training Attendance Sheets, Login Details, Induction Checklist, Staff CPD Records		

Doc. No.	7.2	**Version No.**	2
Last Reviewed	August 2020	**Approved By**	BOM
Next Review	August 2023	**Responsibility**	CH
Procedure Title	7.10 Data Retention and Disposal		
Purpose	To provide assistance and guidance to staff in meeting their obligation in relation to the retention and disposal of data.		
Staff Involved	All Staff		
Procedure	1. Management will: - Ensure all staff are made aware of the records retention schedule so that they know which records the organisation has decided to keep and their personal responsibility to follow the retention schedules. 2. Information users will: - Review records in accordance with the retention schedule when they are no longer required for on-going business or specific legal or regulatory purposes. - Review records at the end of their retention period and arrange for secure destruction, transfer to storage or given a further review date. (Documentation of the disposal or transfer of records will be completed and retained). - Manage electronic records in accordance with the retention schedule. It is recommended that an intended disposal or review date is captured when creating electronic records. 3. All data created and/or received by staff in the course of their duties are retained for as long as they are required to meet the legal, administrative, financial and operational requirements. 4. The final disposal, either through transfer to archives or destruction, is carried out according to the retention schedules.		

	5. Retention periods depend on different criteria, including compliance with legislation and best practice. The retention periods are the minimum time that records should be kept, and are calculated from the end of the calendar month, following the last entry on the record. 6. A records retention schedule will apply to a series of records, and will indicate when eligible records must be destroyed or deleted, and when permanent records are to be archived. 7. In conjunction with the retention periods included in this Policy, the following principles should also be observed: - Be conservative and avoid inordinate degrees of risk. - Consider the consensus of opinion of knowledgeable/experienced people. - Retain a record if it is likely to be needed in the future, and if the potential consequences of not having it would be substantial and are foreseeable at the time. - Apply common sense. 8. Disposal of records must be authorised by a senior manager or the DPO. - Where hard copy records are to be destroyed after the retention period has expired, they should be destroyed using a shredder, or where there is a large amount of records to be destroyed, a professional contractor with expertise in this field should be employed on a confidential basis with the intention that such contractor will oversee the process and issue a certificate of destruction. - A record in the form of a register is to be maintained of all records destroyed, providing verifiable authorised proof of destruction. - The register should be kept in perpetuity and should provide details of all records destroyed, including identifying the name of the person to whom the record relates. - The register should be signed and dated by the person who authorised the destruction of the records. This register should be held in a secure location. - Electronic records should be disposed of as per the retention schedule. - Third parties who have received records should be notified and requested to dispose of those records according to the retention schedule.
Records	Retention Schedule, Disposal Log, Staff CPD Records, Emails

Doc. No.	7.2	Version No.	2
Last Reviewed	August 2020	Approved By	BOM
Next Review	August 2023	Responsibility	CH

7.11 Data Retention Schedule

Record Type	Retention Period	Disposal
Volunteers Records – I-Vol	6 years	Contact individuals for consent to retain. If no consent permanently delete from the system.
Volunteer Involving Organisations Records – I-Vol	6 years or until no longer in existence.	Contact for consent to retain. If no consent permanently delete from the system.
Other Stakeholder Records		
Quality Review Records	Indefinitely	Archive
Human Resource Records		
Applications for a vacant position: - Notification - Copy of advertisements - Job description - Short listing criteria - Candidates not shortlisted - Application forms - CVs - Selection Criteria - Letter of offer - Correspondence to unsuccessful candidates.	1 year	Shred and/or delete
Job Description	3 years after being superseded	Archive
Interview Panel - Marking Sheets - Interviewers notes - Panel Recommendations	2 years	Shred and/or delete.
Personnel Files: - Application and CV - References - Acceptance of Position - Contract of employment - Job description - Performance Appraisals	6 years after employment ends unless required for pension purposes..	Shred and/or delete.

- Support and supervision records. - Attendance records – work - Training and qualification records.		
Leave Records: - Annual leave applications - Sick leave including certificates. - Career break application and correspondence - Jury service. - Compassionate leave.	3 years	Shred and/or delete.
Discipline records and correspondence.	6 years after employment finishes or if involving criminal activity until after the individuals death,	Shred and/or delete.
Insurance policies, Accident reports, Claims correspondence.	Indefinitely	Archive
Financial Records		
Accounts Payable - Invoices - VAT Records - Tax Clearance Certs	Current year + 6 years	Shred and/or delete.
Accounts Receivable - Debtors ledgers - Income listings - Income control accounts - Receipts reconciliation	Current year + 6 years	Shred and/or delete.
Agreements – Rental, Lease, Use, Occupancy	Indefinitely	Archive
Bank Records - Bank Statements - Reconciliation	Current year + 6 years	Shred and/or delete.
Administration Records	Case by Case basis	Archive
Governance Records	Indefinitely	Archive
Health and Safety Records	Indefinitely	Archive
Garda Vetting Records		
1. Vetting invitation information should be deleted from Google Forms after 6 month period.	6 months	Delete

2. Only download one PDF copy of a disclosure from the e-vetting system for processing – Disclosures are only available on the system for 30 days. 3. Permanently delete disclosures from the Download folder on the computer and the sent email once they have been processed – copies are not to be maintained as they are available on the e-vetting system for 30 days.	30 days For length of time it takes to process	

3. Monitoring and Review

Monitoring and Review	The DPO will be responsible for monitoring compliance by carrying out random audits during the year and a scheduled audit annually. The procedures will be reviewed annually or sooner if required. Any issues will be raised at regularly scheduled staff meetings and actioned as required. The policy will be reviewed by the Board every three years, or sooner if required.
Records	Record of Meetings, Audit reports, Document Control Matrix

Appendix 1: Joint Data Controller Agreement

Click image to access document