



Data Protection Policy and Procedures

Version	Approved By	Approval Date	Scheduled Revision Date
1.0	CEO	02.08.13	August 2014
2.0	CEO	16.07.15	July 2018
3.0	Head of Corporate Services	22.01.19	January 2022
4.0	Head of Learning & Growth	24.12.24	December 2027

Contents

- 1. Introduction 3
- 2. Definitions and the Data Protection Principles 3
- 3. Statement of Policy 5
- 4. Disclosure of Personal Information 5
- 5. Handling of Personal Information 5
- 6. Compliance 6
- 7. Staff Responsibilities: Data Storage and Use 7
- 8. Staff Responsibilities: Data Accuracy 8
- 9. Third Party Users of Personal VSS Information 8
- 10. Individuals’ Rights 9
- 11. Making a Subject Access Request 11
- 12. Policy Awareness 11
- 13. Variation 12
- 14. Policy Review 12

1. Introduction

- 1.1. The Data Protection Act 2018 outlines the legal extend to which data can be collected, processed, and used within the UK.
- 1.2. The Victims and Survivors Service (VSS) is fully committed to complying with the General Data Protection Regulations (GDPR) 2018 and the Data Protection Act 2018 (the Act). We will follow procedures to ensure that all employees, contractors, consultants and other parties who have access to any personal or sensitive personal information held by or on behalf of VSS are fully aware of and abide by their duties and responsibilities under the Act.

2. Definitions and the Data Protection Principles

- 2.1. The Act defines a number of key terms as follows:

- **Personal data** - information that relates to an identified or identifiable living individual, or who can be indirectly identified from that information in combination with other information. It includes photographs, email messages and images recorded on CCTV.
- **Special category data (Sensitive personal data)** - also relates to an identifiable living person, but specifically reveals or concerns:
 - Racial or ethnic origin;
 - Political opinions;
 - Religious or philosophical beliefs;
 - Trade union membership;
 - Genetic data;
 - Biometric data (where used for identification purposes);
 - Data concerning health;
 - Data concerning a person's sex life; and
 - Data concerning a person's sexual orientation.

Special category data and criminal office data need more protection because they are sensitive.

- **Data protection principles** – the seven key principles which lie at the heart of the approach to processing personal data;
 - Lawfulness, fairness and transparency
 - Purpose limitation
 - Data minimisation

- Accuracy
 - Storage limitation
 - Integrity and confidentiality
 - Accountability
- **Processing** – in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including
 - collection, recording, organisation, structuring or storage,
 - adaption or alteration,
 - retrieval, consultation or use,
 - disclosure by transmission, dissemination or otherwise making available,
 - alignment or combination,
 - restriction, erasure or destruction.
 - **Data controller** – determines the purposes and means of processing personal data.
 - **Data processors** – are responsible for processing personal data on behalf of a controller.
 - **Data subjects** – are any persons whose personal data is being collected, held or processed.

2.2. The VSS fully supports and complies with the principles of the Data Protection Act (2018) and implementation of General Data Protection Regulation that,

We must ensure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

2.3. The VSS is a listed organisation on the Information Commissioner's Data Protection Public Register.

3. Statement of Policy

- 3.1. The VSS needs to collect and use information about people with whom we work in order to carry out our business and provide our services. These may include members of the public, current, past and prospective employees, clients and suppliers.
- 3.2. In addition, we may be required by law to collect and use information. All personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it is within manual files, in computer records or recorded by any other means.

4. Disclosure of Personal Information

- 4.1. Strict conditions apply to the passing of personal information both internally and externally. VSS will not disclose personal information to any third party unless we believe it is lawful to do so. Respect for confidentiality will be given, where appropriate. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:
 - we have the statutory power or are required by law to do so; or
 - the information is clearly not intrusive in nature; or
 - the member of staff has consented to the disclosure; or
 - the information is in a form that does not identify individual employees.

5. Handling of Personal Information

- 5.1. All VSS staff will, through appropriate training and responsible management:
 - fully observe conditions regarding the fair collection and use of personal and sensitive personal information;
 - meet our legal obligations to specify the purposes for which personal information is collected and processed;
 - collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
 - ensure the accuracy of personal information used;
 - apply strict checks and appropriate data retention schedules to determine the length of time personal information is held;
 - ensure that the rights of people about whom information is held can be fully exercised under the Act;

- respond to subject access requests promptly and within the one calendar month deadline;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without adequate safeguards;
- ensure all personal data is held in line with VSS records management policy.

All staff should be aware that deliberately or recklessly obtaining or disclosing personal data without the consent of the controller is a criminal offence under Section 170 of the Data Protection Act 2018.

6. Compliance

6.1. VSS will ensure that:

- there is always someone with specific responsibility for data protection in the organisation, our DPO – Data Protection Officer
- all staff complete mandatory online data protection awareness as part of their induction and will be directed to data legislation in their induction pack as provided by HR.
- everyone managing and handling personal information understands that they are directly and personally responsible for following good data protection and records management practice;
- only staff who need access to personal information as part of their duties are authorised to do so
- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised
- anyone wanting to make enquiries about handling personal information knows who to speak to and where to seek advice
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are clearly understood and available
- regular monthly review of the Information Assets Register is conducted by the Monitoring and Evaluation team and reported at monthly Operations meetings. In addition to this an annual review will take place once a year by DPO and M&E manager on current personal data processes and how data is handled in the organisation generally.

- processes of handling personal information are regularly assessed and evaluated

6.2. To assist in achieving compliance, the VSS has:

- appointed the Service Development & Reporting Manager with overall responsibility for data protection within the organisation (DPO);
- the co-ordination of FOI requests and Subject Access requests will be carried out by the VSS Risk & Governance Manager, supported by the DPO where required.
- appointed the Data Protection Officer to ensure staff compliance with the data protection principles.

7. Staff Responsibilities: Data Storage and Use

7.1. All staff have a responsibility to protect the personal information held by VSS. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss, disclosure or destruction and in particular will ensure that:

- they are appropriately trained in the handling of personal information;
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically;
- individual passwords are not easily compromised.

7.2. Where data is stored in hard copy (on paper), it should be kept in a secure place where unauthorised people cannot see it.

7.3. These guidelines also apply to data that is usually stored electronically but which has been printed out for some reason:

- When not required, the paper or files should be kept in a locked filing cabinet / drawer / cupboard.
- VSS employees should make sure paper and printouts are not left where unauthorised people could see them (e.g. on a printer / photocopier).
- When no longer required, data printouts should be disposed of securely using the secure disposal units in the VSS office.

- 7.4. Where data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts. The VSS IT system complies with the NICS IT security standards and does not allow the use of removable media.
- 7.5. When working with personal data, VSS employees should ensure the screens of their computers are always locked when left unattended.
- 7.6. Questions about storing data safely can be directed to the Data Protection Officer.
- 7.7. If and when, as part of their responsibilities, VSS staff collect information about other people, they must comply with this policy. No one should disclose personal information outside the commitments made under this policy or use personal data held on others for their own purposes.
- 7.8. When disposing securely of personal data and all other information related to the operations of the VSS, staff must refer to the VSS Data Retention Schedule, which provides guidance on the retention periods applicable to different categories of information.

8. Staff Responsibilities: Data Accuracy

- 8.1. It is the responsibility of all VSS employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- 8.2. Data will be held in as few places as necessary. VSS Staff should not create any unnecessary additional data sets.
- 8.3. VSS staff should take every opportunity to ensure data is updated; for instance, by confirming a client's details when they call.
- 8.4. Data should be updated as inaccuracies are discovered, and incorrect information removed.

9. Third Party Users of Personal VSS Information

- 9.1. Any third parties who are users of personal information supplied by VSS will be required to confirm and demonstrate that they will abide by the requirements of the Act via established and implemented data sharing agreements.

10. Individuals' Rights

10.1. The Act gives individuals certain rights in respect of personal information held about them by others. VSS notes and observes these rights, as set out below.

10.2. Right of Subject Access

10.2.1. Upon making a request in writing, which includes emails, an individual is entitled:

- to be told whether we or someone else on our behalf possesses that individual's personal information; and if so, to be given a description of:
 - a) the personal information;
 - b) the purposes for which it is being processed; and
 - c) those to whom the data are or may be disclosed.

- to be told, in an intelligible manner, of;
 - a) all the information which forms any such personal data (which must be supplied in permanent form by way of a copy, except where this is not possible and would involve disproportionate effort or the data subject agrees otherwise).
 - b) If information is not intelligible (i.e. it is held in coded form), the data subject must be provided with an explanation of that information (e.g. a key to the code); and
 - c) any information as to the source of the information (except where the VSS is not obliged to disclose such information);

10.2.2. We need not comply with the request until we have received the request and the information necessary to meet the request (i.e. in order to satisfy us as to the identity of the person making the request and to locate the information which that person seeks).

10.2.3. We must comply promptly, and no later than one calendar month from receipt of the request, or on receipt of the necessary information. We do not need to comply with a request where we have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed since complying with the last request. What is reasonable will depend upon the nature of the information, the purposes for which the information is processed and the frequency with which the information is altered.

10.2.4. The information given in response to a subject access request should be all that which is contained in the personal data at the time the request was received. Routine amendments and deletion of the information may continue between the date of the request and the date of the reply and, to this extent, the information revealed to the data subject may differ from the information held at the time the request was received. However, we must not make any special amendment or deletion which would not otherwise have been made and the information must not be tampered with in order to make it acceptable to the data subject.

10.2.5. **Disclosure of third party data:** In some cases, we may find that in complying with a subject access request, we will disclose information about a person other than the data subject who can be identified from that information, including the situation where they can be identified as the source of the information. In such cases, we can only disclose that information where:

- the third party has consented to its disclosure; or
- it is reasonable in all the circumstances to comply with the request without the consent of the other person.

10.2.6. If we are satisfied that the data subject will not be able to identify the other individual from the information requested, taking into account any other information which, in our reasonable belief is likely to be in (or come into) the possession of the data subject, then we must provide the information.

10.2.7. **Failure to comply with a subject access request:** If a data subject believes that we have failed to comply with a subject access request in contravention of the 2018 Act, they have the right to complain to VSS through our Complaints Procedure.

10.3. Right to Prevent Processing Likely to Cause Damage or Distress

10.3.1. This right gives the data subject the right to serve a written notice on a data controller (in this case, VSS) to cease or not to begin even the lawful processing of personal data about them if the processing is 'unwarranted as causing or being likely to cause significant damage or distress to him or another.'

10.3.2. Any dispute between the data controller and the data subject is resolvable in Court. This right is not available where the personal information is being processed in pursuance of a statutory duty.

10.3.3. The Secretary of State has the power to make further exemptions by order, but has indicated that, in view of the high threshold for the data subject who is applying for the prohibition, the office is unlikely to provide an exemption in the absence of a very strong case.

10.4. **Right to Prevent Processing for the Purpose of Direct Marketing**

10.4.1. An individual is entitled, by written notice, to require an organisation to cease or not begin processing his/her personal information for the purposes of direct marketing and may apply to court for an order if the data controller fails to comply.

10.4.2. Members of the public who do not wish to receive unsolicited mail from companies, charities, etc. can register with the Mailing Preference Service. Further information on this service can be found on their website at www.mpsonline.org.uk.

11. **Making a Subject Access Request**

11.1. To make a subject access request to VSS, please submit the details of the request to:

Risk & Governance Manager
Victims and Survivors Service
1st Floor, Seatem House
28-32 Alfred Street
Belfast
BT2 8EN
Email: enquiries@vssni.org
[Telephone: 028 9027 9100](tel:02890279100)

11.2. For further information and details on Subject Access Requests please refer to the VSS Data Protection Subject Access Request Procedure complying with the Data Protection Act (2018).

12. **Policy Awareness**

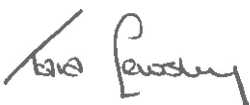
12.1. All new members of staff and interested third parties will be directed to a copy of this policy statement. Existing staff and any relevant third parties will be advised of the policy which will be posted on our internet site, as will any subsequent revisions. All staff and relevant third parties are to be familiar with and comply with this policy at all times.

13. Variation

13.1. VSS reserves the right to vary this Data Protection Policy as it deems appropriate to include compliance with any legal requirements.

14. Policy Review

14.1. This policy will be reviewed in 3 years' time, or sooner, if required.

Approved: 

Tara Lewsley
Head of Learning & Growth

Date: 24/12/2024