Data Protection Policy

Policy number:		Version:	1.9
Date created:	23rd September 2016	Date of last update:	June 2020
Responsible owner:	Jenny Owen	Reviewed:	June 2020

Purpose

This Policy describes how we will collect, handle, transfer, store, and protect Personal Data in compliance with the law and our own data protection standards globally. For the purpose of this Policy, Personal Data means any information relating to any individual (who are referred to as "Data Subjects" in this policy).

VSO needs to collect, handle, transfer, and store information about Data Subjects in order to carry out our work to achieve VSO's mission to bring people together to fight poverty.

We have adopted this Policy to ensure that we protect Data Subjects from breaches of confidentiality and protect their legal rights.

The VSO International Board is fully committed to ensuring effective implementation of this Policy.

Who does this Policy apply to?

This policy applies to all VSO People i.e. employees, volunteers, contractors, business contacts, consultants, suppliers, temporary staff and other people at VSO worldwide including supporter groups. This includes the Kingston Office, all branches of VSO, and all locally registered VSO NGOs globally. This includes VSO Ireland and VSO Netherlands and VSO's International Board.

Dissemination and Enforcement

Breach of this Policy, will be taken very seriously and appropriate action may result. This may include termination of contract and in the case of employees, disciplinary action, which may result in summary dismissal in the most serious cases.

Audit

To confirm that an adequate level of compliance is achieved by all VSO People in relation to this Policy the VSO Internal Audit Function will include compliance checks as part of the regular schedule of internal audits including:

- Assignment of responsibilities

- Awareness and training
- The effectiveness of VSO's data protection operational practices such as maintaining Data Subjects' rights, personal data incident management, data privacy notices, procedures for redressing poor compliance and personal data breaches, accuracy of personal data being stored and handling of Subject Access requests.

Roles and Responsibilities

International Board

This Policy is approved by the highest level of governance within VSO, its International Board, which has the responsibility of ensuring that VSO meets its legal obligations.

Data Protection Officer

The VSO Data Protection Officer is the General Counsel and Company Secretary, who reports to the CEO and so as to ensure independence, to the Chair of the VSO International Board and is responsible for:

- Keeping the Board updated about its data protection responsibilities
- Reviewing all data protection procedures and related policies annually
- Arranging data protection training for those affected by this policy
- Handling requests from Data Subjects to exercise their individual rights (for example, to see or remove their Personal Data)
- Handling data protection questions
- Checking and agreeing contracts or agreements with third parties that may handle Personal Data
- Approving data protection statements attached to e mails, letters and other communications
- Handling complaints from Data subjects

Infrastructure, Security and Compliance Manager

The Infrastructure, Security and Compliance Manager is responsible for:

- Ensuring that all system, services and equipment used for storing Personal Data meet acceptable standards
- Performing regular checks and scans to ensure security hardware is functioning properly
- Evaluating the technical suitability of third party services VSO may use for providing storage or processing of Personal Data.
- Maintaining Data Breach Monitoring solutions.

All VSO managers

All managers must ensure that everyone within their area is aware of and complies with the contents of this Policy and related policies.

All VSO People

All VSO People are responsible for being aware of and following this policy.

Training

All VSO People at all levels are required to carry out VSO's mandatory Data Protection Training Module every year.

Data Protection Principles

VSO has adopted the following 6 principles to govern its collection, use, retention, transfer, and destruction of Personal data. These are:

1. **Lawfulness, fairness and transparency**

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

VSO will only collect and use Personal Data in a consistent, fair and lawful way. Data Subjects will be informed about how VSO will store and use Personal Data at the time of collection.

VSO will require a standard statement to be included in all written requests for Personal Data directing Data Subjects to our privacy notice, and a similar verbal script will be used for phone data collection.

2. **Purpose limitation**

Personal data shall be collected for specified, explicit and legitimate purposes only and not further processed in a manner that is incompatible with those purposes

VSO will always specify how it will use Personal Data and it will never process it in a manner incompatible with that purpose. You should speak to your manager or the Data Protection Officer if you are unsure about whether your use of Personal Data is compatible with the original purpose for which the data were collected.

VSO will never use Personal Data collected for purposes of a volunteer's or employee's contract and then use it for marketing or fundraising without Explicit Consent.

Where VSO intends to use Personal Data for its main purposes, sending volunteers overseas, campaigning, educational work in volunteers' home countries or overseas, we will rely on one of the following lawful conditions:

- the use of the Personal Data is necessary in order to perform a contract we have with the Data Subject; or
- VSO considers it has a legitimate interest in processing Personal Data in connection with its work it will carry out a balancing exercise to ensure that the fundamental rights and freedoms of the Data Subject are not overridden by the interests of VSO.

If VSO wishes to make other uses of Personal Data by VSO Data Subjects they will be given an informed choice to give or withhold Consent.

VSO will strive to ensure that Personal Data collection is accurate and complete as possible at the point of collection.

In some limited circumstances it is permissible for Personal Data to be used and shared without the consent of Data Subject for example for purposes of crime detection, apprehension or prosecution of offenders, assessment of taxes or duties and by Court Order. In such case disclosure will only be made by VSO to the limited extent necessary to meet our legal obligations or in an emergency situation to protect someone's vital interests.

3. Data minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

We will not collect retain or process more Personal Data than is necessary for processing in accordance with this policy.

VSO People must only use Personal Data if it is necessary for their work for or on behalf of VSO. Personal Data must not be used for any reason unrelated to someone's authorised duties.

4. Accuracy

Personal Data shall be accurate and, where necessary, kept up to date.

Personal Data will be kept up to date and accurate by VSO which means that VSO will operate the procedures attached to this Policy to ensure Personal Data is always kept up to date and to identify and address any out of date, incorrect and redundant Personal Data.

5. Storage limitation

Personal Data shall be kept for no longer than is necessary for the purposes for which the personal data are processed.

VSO will not store any Personal Data beyond what is necessary (including for the purpose of satisfying any legal, accounting or reporting requirements) and in accordance with the VSO Data Retention Policy. (Link)

6. Integrity and confidentiality

Personal Data shall be 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.

Personal Data may be stored in many ways such as databases, structured manual filing systems or electronic filing systems.

VSO will ensure that adequate technical and organisational measures are in place to ensure that Personal data is protected.

All VSO People must take reasonable and appropriate security measures when they process Personal Data on behalf of VSO and must follow procedures in place from time to time.

Children's Personal Data

VSO will not usually ask children to consent to the processing of their personal data and will seek and obtain written consent from the person with parental responsibility for their child when consent is required for compliance with this Policy.

In limited circumstances where processing of Personal data of a child may be lawful without parental consent but guidance and approval must first be obtained from the Data Protection Officer.

Treatment of Sensitive Personal Data

Sensitive Data is Personal data relating to a Data Subject's:-

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- Trade Union membership
- Physical or mental health
- Sex life
- Sexual orientation
- Criminal convictions, offences or related security measures.
- Genetic data
- Biometric data

We will usually only collect Sensitive Personal Data with the Data Subject's unambiguous and specific freely given consent.

We may use VSO People's Sensitive Personal Data in order to carry out our obligations or exercise our rights in the field of employment, social security, or social protection law. Where employees or volunteers are working with children and/or vulnerable adults, we may process Sensitive Personal Data about criminal convictions as part of a criminal records check carried out for reasons of substantial public interest.

In an emergency, we may need to use Sensitive Personal Data to protect someone's vital interests if the individual is physically or legally incapable of giving their consent.

We limit access to all Sensitive Data to our medical and safeguarding teams and to those of our staff with a strict need to know.

Transfer of Personal Data

VSO will make sure that transfer of Personal Data will only take place where it is protected in the country it is transferred to or the Data Subject has given Consent to the proposed transfer. VSO People should speak to their manager or the DPO if they are unsure about transferring Personal Data to a country outside the European Economic Area (EEA).

Privacy Notices

VSO will include a privacy notice and online Cookie Notice on each external website it publishes including the ICS website. The privacy notice includes information about who we are, how we process Personal Data and the steps we take to protect Personal Data. Any changes in the wording of such notices must be approved by the Data Protection Officer and reviewed annually.

If we collect Personal Data from a third party or from a publicly available source, we must provide the Data Subject with a copy of our privacy notice as soon as possible and not later than one month after we collect their Personal Data.

Data protection impact assessments

VSO must undertake a data protection impact assessment (DPIA) if we plan to process Personal Data in a way that is likely to result in a high risk to Data Subject. It is also good practice to conduct a DPIA for major projects which will require us to process Personal Data.

We will usually conduct a DPIA when we implement major system or business change programs which involve processing Personal Data, such as:

- use of new technologies (programs, systems or processes), or changing technologies
- automated processing (including profiling) such as the use of Personal Data to evaluate, analyse or predict personal preferences, interests, or behaviour
- large-scale processing of Sensitive Personal Data;
- large-scale, systematic monitoring of a publicly accessible area.

You should contact the Data Protection Officer if you think it may be necessary to conduct a DPIA in relation to work that you are carrying out for VSO.

Data Subject Rights

VSO will operate systems to respond and facilitate the exercise of Data Subjects' individual rights in respect of their Personal Data. These are set out in the Individual Rights Policy which includes the procedures to be followed if any individual makes a request to exercise any of their individual rights.

Complaints Handling

Complaints from Data Subjects about the processing of their Personal Data are to be handled in accordance with the Procedures attached to this Policy.

Breach Reporting

If any VSO Person suspects that a Personal data Breach has occurred they must IMMEDIATELY notify this in accordance with the Procedures attached to this Policy. Data breaches may have to be reported to the Information Commissioners office or notified to the Data Subject(s) involved within **72 hours**. The Data Protection Officer will initiate a team to coordinate and manage the response in accordance with the timelines required by the Information Commissioner's Office.

Notification

VSO will maintain up to date Notifications with the Information Commissioner's Office and elsewhere as required by law.

Related Documents and Procedures

- Data Retention Policy and Matrix
- Complaints handling - Supporter Care
- Individual Rights Requests
- Incident Management Plan/Breach Response Procedure
- Privacy Notice

Data Retention Policy

Introduction

This policy supports the organised creation, retrieval, proper storage and preservation of VSO's essential records, and to enable identification and destruction of information where there is no continuing business, legal or historical significance.

This policy also helps us to comply with legal requirements and maintain records of potential interest to VSO People and members of the public. Records of activities and achievements contain accumulated experience, expertise and knowledge.

This policy applies to all personal data held by VSO, both physical and electronic.

Data Retention Responsibilities

Data Protection Officer (DPO)
As part of its ongoing commitment to the highest standard of data protection, VSO has a DPO with expert knowledge of data protection law. The core functions of the DPO are:

- To inform and advise VSO on its data protection obligations.
- To monitor VSO's compliance with this policy.
- To provide advice.

VSO's DPO is currently Jenny Owen who can be contacted at:
jenny.owen@vsoint.org or dataprotection@vsoint.org,
VSO International, 100 London Road, Kingston upon Thames, KT2 6QJ, UK.

Executive Board
The Data Retention Policy is maintained by VSO's DPO and is approved by the Executive Board.

All
Everyone has a responsibility to make themselves familiar with this policy and related policies. Updates to the data retention schedule should be submitted to the DPO.

Principles

VSO has 3 key principles that determine what information needs to be retained:

1. **Information that needs to be kept by law**

VSO is required to keep certain information by law, for example, the Health and Safety at Work Act.

2. **Information that has ongoing business value**

This is information that is of value to VSO, which is needed for both day to day activities and longer term strategic planning.

3. **Information that is of historical value**

Information of historical value is that which reflects the 'what, why and how' of VSO. This will include significant policy documents, records of significant decisions and documents about notable events, persons or public issues.

There are limits as to how long information needs to be kept for. Retaining information for longer than necessary creates cost for the organisation. There is the actual cost of storing information that is no longer needed either in offsite archives or within our IT infrastructure, as well as the cost to the organisation of not being able to use our information resources effectively to support us in our work. A key principle of data protection is that personal data must not be kept for longer than is necessary. This means as an organisation we must:

- review the length of time personal data is kept;
- consider the purpose for which the information is held to decide how long to retain it;
- securely delete information that is no longer needed; and
- update, archive or securely delete information if it goes out of date.

Retention schedule

The retention schedule lists the documents and the period for which we intend to keep them. The retention schedule is not an exhaustive list but if a document is missing, please inform the DPO.

Destruction

At the end of the retention period, all documents should be destroyed as follows:

- Physical documents should be destroyed securely (crosscut shredding or licensed secure disposal company).
- Electronic documents should be deleted and removed from recycling bins.
- Automated purge routines will be used to remove records from databases and IT systems (such as SharePoint, Salesforce, Raisers Edge etc). This will be managed by IT.

In some circumstances (such as legal action or police investigation), VSO will be required to provide all relevant documentation. This means these documents must not be destroyed until the legal action/investigation has concluded. If anyone receives a request for information in these kinds of circumstances, they must inform the DPO as soon as possible.

The DPO will promptly inform all staff of any suspension in the further disposal of documents.

Page Break

Data protection – incident management procedure

Introduction

Every care is taken to protect personal data from incidents which could lead to a data protection breach or compromise security.
Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs. The objective of this procedure is to contain any breaches, to minimise the risk associated with any breach and consider what action is necessary to secure personal data and prevent further breaches.
This policy relates to all personal and sensitive data held by VSO regardless of format.
This policy applies to all volunteers and staff (including temporary and casual staff), agency workers, contractors, consultants, suppliers and data processors working for, or on behalf of VSO.

Types of Breach

An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data (either accidentally or deliberately) and cause damage to VSO's information assets and/or reputation.
An incident includes but is not limited to the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper records).
- Equipment theft or failure.
- Unauthorised use of, access to or modification of data or information systems.
- Unauthorised disclosure of sensitive / confidential data.
- Hacking or phishing attack.
- Human error.
- Information obtained by deception.

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

Reporting an incident

Who should report an incident?
Any individual who accesses, uses or manages personal or sensitive information is responsible for reporting any actual or suspected data breach or information security incident immediately to the

Data Protection Officer and the data protection mailbox: Jenny Owen (jenny.owen@vsoint.org) / dataprotection@vsoint.org

What to report:

As much information as possible should be included when reporting including:

- When the breach occurred (dates and times).
- Where the breach occurred.
- How the breach occurred.
- Name, location and job title of the person reporting the breach.
- The nature of the information which has been compromised.
- Who was involved.
- Any other relevant information.

When to report:

As soon as possible! If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. **If in doubt report it!**

What happens next?

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, appropriate steps will be taken immediately to contain the breach.

The DPO will call upon various members of staff to form a team to handle the breach. The team will include, at a minimum:

- IT
- Comms
- Human Resources
- Management Liaison

An initial assessment will be made by the DPO in liaison with relevant staff to establish:

- the severity of the breach
- who will take the lead investigating the breach (this will depend on the nature of the breach - in some cases it could be the DPO).

The DPO, in liaison with relevant staff, will determine suitable action to be taken to resolve the incident.

Investigation and risk assessment

An investigation will be undertaken by the DPO or an appointed member of staff immediately and wherever possible within 24 hours of the breach being discovered / reported.

The DPO and relevant staff will assess the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will look into:

- the type of data involved
- its sensitivity
- the protections in place (e.g. encryptions)
- what happened to the data - has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who was involved, number of individuals involved and the potential effects on those data subject(s)

- whether there are wider consequences to the breach.

The incident will be logged on the Data Breach spreadsheet on Sharepoint here: Data Breach Log

Notification

The DPO will determine who needs to be notified of the breach by considering:

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Would notification help VSO meet its obligations under the seventh data protection principle;

The DPO will report the breach, if required, to the ICO and act as the point of contact.

The DPO may be required to inform others about the breach such as:

- The police
- Any individual directly affected by the breach

The DPO must consider notifying third parties such as the insurers, bank or credit card companies, the Charity Commission and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. The DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact VSO for further information or to ask questions on what has occurred.

All actions will be recorded by the DPO.

Testing

Annually the DPO will gather together the relevant people and run through a test scenario to ensure the Incident management procedure is functional. Results of this will be recorded and stored on Sharepoint.

Reflection

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie any further potential weak points
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by VSO.

Responsible owner:	Jenny Owen	Version:	1.9
Date created:	13th June 2018	Date of last update:	June 2020
Updated by:	Jenny Owen		