VSGWL Policy

Personal Data Protection
(Collection, storage, retention, destruction, usage and privacy)

Introduction

We hold personal data about our board, employees, volunteers, members, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understands the rules governing their use of personal data to which they have access in the course of their work.

This policy applies to the board, all staff and volunteers. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet, social media and email use. We may supplement or amend this policy by additional policies and guidelines from time to time.

This policy requires staff to ensure that the Data Protection Officer (DPO), the CEO, be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice; • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests; • Ensuring policies are adhered to (such as policies covering email and internet use); • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information; • Investigating complaints; • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments; • Monitoring staff conduct, disciplinary matters; • Marketing; and • Improving services.

Personal data	Information relating to identifiable individuals, such as job applicants, board members and applicants to the board, current and former employees, placements, interns etc, volunteers, members and suppliers. Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data will be strictly controlled in accordance with this policy. This would also include any staff grievance and disciplinary matters.

Who is responsible for this policy?

Our Data Protection Officer (DPO), the CEO, has overall responsibility for the day-to-day implementation of this policy.

The Data Protection Officer's responsibilities:

- Keep the board updated about data protection responsibilities, risks and issues;
- Review all data protection procedures and policies on a regular basis;
- Arrange data protection training and advice for all staff and volunteers and any others included in this policy;
- Answer questions on data protection from staff, board members and other stakeholders;
- Ensure individuals such as employees, volunteers and members who wish to know which data is being held on them by VSGWL are responded to;
- Ensure any third parties that handle our data, any contracts or agreements regarding data processing, adhere to VSGWL policy;
- Ensure all systems, services, software and equipment meet acceptable security standards;
- Ensure security hardware and software is checked and scanned regularly to ensure it is functioning properly, this includes any cloud services;
- Ensure Privacy Impact Assessments and carried out before any changes to IT systems;
- Approve data protection statements attached to emails and other marketing copy;
- Ensure data protection queries from members, the sector, funders and other stakeholders are addressed; and
- Ensure all marketing initiatives adhere to data protection laws and VSGWL Data Protection Policy.

The processing of all data must be:

- Fair and lawful, in accordance with individuals' rights
  (This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.);
- Necessary to deliver our services;
- In our legitimate interests and not unduly prejudice the individual's privacy;
- We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented;
- All staff that is responsible for processing personal data will be aware of the conditions for processing; and
- The conditions for processing will be available to data subjects in the form of a privacy notice.

VSGWL will abide by any request from an individual not to use their personal data for direct marketing purposes. Staff and volunteers will notify the DPO about any such request.

VSGWL will not send direct marketing material to someone electronically (e.g. via email, text, social media etc) unless VSGWL has an existing relationship with them in relation to the services being marketed.

Contact the DPO for advice on direct marketing before starting any new direct marketing activity.

VSGWL Membership Form and website contain a **Privacy Notice** to members and users on data protection.

The notice:

- Sets out the purposes for which we hold personal data on board members, employees, volunteers, members, the wider Sector, funders and stakeholders;
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers; and
- Provides that data subjects have a right of access to the personal data that we hold about them.

Personal data

Sensitive data. In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, CEO. This will be held in the Data Register.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Criminal record checks

Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability/subject access requests

Under the Data Protection Act 1998, a data subject is entitled, subject to certain exceptions, to request access to information held about them.

Subject access requests must be referred immediately to the DPO.

The data subject has the right to receive a copy of their data in a structured format. These requests will be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.

A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed and VSGWL must comply with the request. An erasure request can only be refused if an exemption applies.

Please contact the DPO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Data security

VSGWL will keep personal data secure against loss or misuse.

Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it;
- Printed data should be shredded when it is no longer needed;
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords;
- Data stored on CDs or memory sticks must be locked away securely when they are not being used;
- The DPO must approve any cloud used to store data;
- Servers containing personal data must be kept in a secure location, away from general office space;
- Data should be regularly backed up in line with the company's backup procedures;
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones;
- All servers containing sensitive data must be approved and protected by security software and strong firewall; and
- When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data retention

VSGWL will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but will be determined in a manner consistent with VSGWL data retention guidelines.

Data Type	Retention Period
Employee / volunteer personnel files / director files	Up to 6 years after the end of employment
Recruitment and selection procedures and results	6 months from date of result
Discipline	A copy of the Informal Action Note will be kept on file but will be disregarded for disciplinary purposes after 6 months. The final written warning will normally be disregarded for disciplinary purposes after 12 months.
Grievance	Up to 6 years after the end of employment.

Dismissal	Up to 6 years after the end of employment
Financial records	7 years after the end of the year to which they relate
Insurance certificates	40 years
Members	Annual membership. Records kept for 3 years.
Complaints records	3 years
VSGWL (historical information)	Indefinite

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

The board, all members of staff and volunteers have an obligation to report actual or potential data protection compliance failures to the DPO. This allows VSGWL to:

- Investigate the failure and take remedial steps if necessary; and
- Maintain a register of compliance failures.

Training

The board, all staff and volunteers will receive training on this policy. New starts will receive training as part of the induction process.

Further training will be provided at least every two years, or whenever there is a substantial change in the law, or our policy and procedure. This will be recorded in our Training Register.

Training will be provided through in-house seminars and on-line on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

Monitoring

The policy will be monitored regularly to make sure it is being adhered to.

Consequences of failing to comply

VSGWL takes compliance with this policy very seriously. Failure to comply puts both individuals and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Tel: 01506 650111

Email – vsg@vsgwl.org

Date of Adoption 16/8/19

Date of Review 16/8/21

Authorised D Evans

Title Chair Date 16/8/19