Data Protection and GDPR Policy

Reviewed:	September 2025
Next Review Date:	September 2026
Reviewed By:	Molly Elliott

Induction

We hold personal data about our employees, clients, supplier and other individual for a variety of business purposes.

The policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy required staff to ensure that the Data Protection Officer be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps addressed.

Definitions

Business Purposes	The purpose for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes included 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 business 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, security vetting, credit scoring and checking - 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 our business - Improving services

Personal Data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. 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 race 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 should be strictly controlled in accordance with this policy.

Scope

The policy applies to all staff. You must be familiar with this policy and comply with its terms

The policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our Data Protection Officer, Molly Green has overall responsibility for the day-to-day implementation of this policy.

Our Procedures

Fair and lawful proceedings

We must process personal data fairly and lawfully 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.

The Data Protection Officer's Responsibilities:

- Keeping the board updated about data protection responsibilities, risk and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff and board members

- Responding to individuals such as clients and employees who wish to know which data is being held on them by VS
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Department

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking the scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party service, such as cloud services the company is considering using to store or process data

Responsibilities of the Marketing Manager:

- Approving data protection statements attached to email and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy.

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities

Our Terms of Business contains a Privacy Notice to clients on data protection. The notice:

- Sets out the purpose for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right to access to the personal data that we hold about them.

Sensitive Personal 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 relation to them. If you believe that information is inaccurate you should record the face that the accuracy of the information is disputed and inform the DPO, Molly Green.

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 Compliance Team who update your records.

Data Security

You must 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 now 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.
- The DPO must approve any cloud used to store data.
- Servers containing personal data must e 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 unless it is password protected in line with policy and for use only within the objectives of this policy
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Retention

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

Transferring Data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside of the UK without consulting the DPO.

Subject Access Requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information help about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

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.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purpose and notify the DPO about any such requests.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

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

Training

All staff will receive training on this policy. New starters will receive training as part of their induction process. Further training will be provided at least every year or whenever there is substantial change in law or our policy and procedure.

Training is provided through an in-house training site 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.

COVID-19

During the Coronavirus pandemic, we have always followed government and APSCo advice.

As an alternative to face-to-face interviewing, video interviewing has been introduced as a measure whist social distancing was in place.

Consultants are required to use Microsoft Teams for interviews with a secure invitation link emailed only to the applicant before their meeting. The recording of interviews is solely for audit purposes to verify original documents which will provide a secure stream link once the recording has finished. Any recordings or documents provided during the registration will be saved within a candidates record which as mentioned above is a password-protected CRM system giving only the consultants and relevant admin access to the candidates records.

For further information around the security of Microsoft Teams, please follow the links below:

https://www.microsoft.com/en-gb/privacy/privacystatement

https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/06/microsofts-commitment-privacy-security-microsoft-teams/#%3A~%3Atext%3DWe%20provide%20privacy%20and%20security%20controls%20for%20video%20conferences%20in%20Teams%26text%3DWhen%20recording%20a%20meeting%2C%20all%2Cpeople%20invited%20to%20the%20meeting

As with all data, candidates can request for their data to be removed at any time, which will include deleting the link to their interview recording.

GDPR Provision

Being transparent and providing accessible information to individuals about how we will use their personal data is important for VES. The following are details on how we collect data and what we do with it:

What information is being collected?

CVs and personal details including phone numbers, email addresses, addresses and date of birth. When someone comes in to register, we are obliged to collect safeguarding documents such as ID, proof of address, proof of NI number, DBS and qualifications certificates. Further information on this is held in our data retention policy.

Who is collecting it?

The data is collected by VES staff including Recruitment Consultants, Compliance Officers, Payroll/Accounts and Directors.

How is it collected?

VES obtains data from a variety of courses, these include:

- Through our website
- Through our social media including Facebook, X, Instagram and LinkedIn
- Through phone enquires
- Through job applications
- Through CV watchdogs i.e. when a CV is uploaded

Why is it being collected? How will it be used?

We use data always with the goal of obtaining work for an individual, with their permission details of experience and work history will be passed to our clients.

Data will be stored on our internal systems which will always ben password encrypted, all paper files will be kept in locked cabinets.

Who will it be shared with?

We use data always with the goal of obtaining work for an individual, with their permission details of experience and work history will be passed to our clients.

What will be the effect of this on the individuals concerned?

Once data is added to our database, the individual can expect to receive a notification within one month explaining where we obtained the data from a link to this notice.

We use data always with the goal of obtaining work for an individual, with their permission details of experience and work history will be passed to our clients.

We may contact you via phone or email to inform you of:

- Job Opportunities
- Obtain your availability to work
- Events we think you might be interested
- Confirmation of work
- CPD Opportunities
- Changes within our businesses e.g. Consultant changes, pay changed, opening hours etc.

This will be no more than once a week although if you are in a placement and require information associated with that it may be more regular.

Is the intended use likely to cause individuals to object or complain?

We believe that adhering to this processing policy means that all data is dealt with in an appropriate way. Should individuals wish to complain they may do so in line with our complaints policy. An individual may unsubscribe at any time by emailing dataprotection@vesrecruitment.co.uk.

Conditions for Processing

We will ensure any use o personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for Personal Data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal Record Checks

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

Data Portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden, and it does not compromise the privacy of their 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 help on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by Design and Default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

International Data Transfer

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data Audit and Register

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

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

VES procedure is as follows:

1) As soon as the breach is identified the employee must notify the DPO.
2) The employee will make a note of the breach on the relevant record in our database system
3) The DPO will record the breach on the data breach spreadsheet in the HR Brive and notify the directors.
4) The Directors will decide the appropriate approach and action
5) The DPO will follow up with the directors and record actions taken on the spreadsheet.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirements may lead to disciplinary action under our procedure which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.