about the organisation, its products and services, its customers and suppliers.

PRINCIPLES OF DATA PROTECTION

Any personal data which 6RO,QVWLWXWH collects, records or uses in any way, whether it is held on paper, on computer or other media, will have appropriate safeguards in place to ensure that we comply with the Act. Sol Institute fully endorses and adheres to the eight principles of the Act, which state that personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed.
2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Shall be accurate and, where necessary, kept up to date.
5. Processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Shall be processed in accordance with the rights of data subjects under this Act.
7. Shall be protected against unauthorised or unlawful processing, against accidental loss or destruction of, or damage to, personal data by appropriate technical and organisational measures.
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Sol Institute are committed to upholding data protection law and we employ, policies, procedures, training and systems as necessary for full compliance.

DATA MANAGEMENT

Information we hold

Sol Institute keeps personal data to:

- Administer programmes to comply with our contractual requirements.
- To provide an effective service to customers by identifying their needs and managing their progress.
- Meet awarding body requirements in relation to achievement of qualifications by learners.
- To claim relevant funding for achievements with customers attending funded programmes.
- Manage the recruitment, employment and termination of employment of our staff.

The type of data may include (but is not limited to) personal demographic and contact information e.g. names, addresses, nationality, date of birth; references; health and disability information; educational attainment; financial information relating to employment or a service we are providing to customers; information about an individual's performance; attendance records; disciplinary records.

Confidentiality

All personal data will remain confidential. Only people specifically required and entitled to access this information to fulfil their job function may do so, and are required to maintain its confidentiality at all times. All other employees are prohibited from accessing, reading, copying or in any other way dealing with such information. From time to time, we may need to disclose some information to relevant third parties e.g. where requested by the data subject for the purpose of giving a reference, or to help a customer into education or work. Prior to disclosure – unless it is a legal obligation e.g. data required by HM Revenue & Customs, a contractual obligation placed upon us by a service commissioner that is covered by alternative legislation – data subjects will be fully informed of the personal data that is being disclosed, the reasons for the disclosure, and the way(s) in which it will be processed. There may be occasions when data subjects are required to sign a Confidentiality and/or Data Sharing Agreement giving consent to the sharing of some information with other parties. Data subjects can withdraw their consent to share information at any time.

We may occasionally contact individuals by email, mail or telephone with details of our products and services. Recipients wishing to opt out of receiving this information should simply follow the process highlighted in the email to opt out of marketing.

Handling Data

Sol Institute will ensure that all staff comply with the following when processing and/ or transmitting personal data:

- When we collect any personal data we will inform individuals why we are collecting it and what we intend to use it for.
- Personal data must be transmitted over secure networks only – transmission over unsecured networks is not permitted in any circumstances.
- Documents containing personal data must be password protected.
- Personal data contained in the body of an email, whether sent or received, must only be emailed via secure systems with appropriate encryption and security.

- Personal data in the body of an email should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated with the email should also be deleted.
- Where personal data is to be sent by fax the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
- Where personal data is transferred in hardcopy it should be passed directly to the recipient or posted using a recognised secure postal carrier. Using an intermediary is not permitted.
- All hard copies of personal data must be stored securely in a locked box, drawer, cabinet or similar.
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet.
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.

DATA SUBJECT ACCESS

Rights Of Data Subjects

Data subjects have the right to:

- access to a copy of the information comprised in their personal data within 40 days of making a request;
- object to processing that is likely to cause or is causing damage or distress;
- prevent processing for direct marketing
- object to decisions being taken by automated means
- in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- and claim compensation for damages caused by a breach of the Act.

Subject Access Requests

Individuals who want to see a copy of the information an organisation holds about them must write to the Data Controller requesting this information, including sufficient detail to enable their identity to be confirmed and the data to be identified. A fee of £10 must be submitted with the request.

In response to a compliant request, the following information will be provided:

- Whether any personal data is held.
- A description of any data held.
- The reason it is being processed.
- Details of any third-party organisations that the data has been passed to.
- Details of the source of the data where available.
- A copy of information comprising the data including details of any technical terminology or codes.

Data that is exempt from the right of subject access will not be supplied. This may include information relating to crime prevention and detection; negotiations with the subject; confidential references supplied by Success Tuition and Training Centre.

We will respond to all subject access requests promptly and in any event within 40 calendar days of receiving it.

Sol Institute will record any subject access requests in a Subject Access Log in accordance with the Information Commissioner's guidelines.

RESPONSIBILITIES

- All staff and partners working on behalf of Sol Institute are responsible for ensuring data is collected, stored and handled appropriately in line with this policy.
- Board Members are responsible for ensuring the Data Protection Policy is appropriate, reflects legislative requirements and good governance practices, and that Sol Institute meets its legal obligations.
- Data Controller is responsible for ensuring all staff are appropriately trained, advising individuals about implementation of the policy, dealing with Subject Access Requests, and ensuring Sol Institute registration with the Information Commissioner's Office is updated in line with our legal obligations.

MONITORING AND REVIEW

The effectiveness of this policy will be monitored by the Director of Operations at Sol Institute to ensure compliance with data handling and security.

This policy will be reviewed annually by the Data Controller or more frequently if legislation and/or best practice changes, in order to ensure it continues to meet current legislative requirements, adopts emerging best practice, and continues to be effective and relevant to the wider business.

The Data Controller will report back to the Board on the performance of the policy with recommendations for improvement if required. Any changes to the policy will be communicated to all employees.