Data Protection Policy

Aims

The company needs to keep certain information on Learners and Centres in order to lawfully carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the aims of GDPR. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organization, including the use of IT equipment and software.

This policy covers staff and volunteers.

Definitions

In line with the principles of GDPR, the company will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and

- the right not to be subject to automated decision-making including profiling.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

For the purposes of International trade, our lead data protection supervisory authority is the ICO in the UK.

Special category data is defined as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing 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.

Personal data breaches are a breach in security leading to an accidental or unlawful sharing, dissemination, destruction, loss or alteration to personal or special category data. Examples could include:

- loss or theft of a device;
- inappropriate access by a staff member;
- human error;
- hacking or phishing.

Company Responsibilities

The company has three legal bases for processing data:

- **Consent** – for example for marketing purposes;
- **Performance of a contract** – for example training employees of an organisation;
- **Legitimate interest** – for example when a learner requests training or a qualification.

Notification

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Protection Officer within our organisation as specified in our notification to the Information Commissioner is Richard Curtis.

Data Protection Impact Assessments

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

These will be undertaken by the development team with the Data Controller.

If a DPIA indicates that the data processing is high risk, and the company cannot sufficiently address those risks, the Data Protection Officer will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Implementation

We will ensure that:

- Everyone managing and handling personal information will be given this policy and trained to handle the data.
- Staff are given annual refreshers of their data protection responsibilities and malware identification training (and more frequently if a risk is identified);
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.

Queries about handling personal information will be dealt with swiftly and politely.

Staff Training

Induction training for staff will cover:

- Data collection and processing
- Personal Data Guardianship Code
- Data storage
- Data sharing
- Use of IT, passwords and WiFi
- Protecting personal data
- Policy

Refresher training for staff will cover:

- Personal Data Guardianship Code
- Data storage

- Data sharing
- Use of IT, passwords and WiFi
- Protecting personal data
- Policy updates

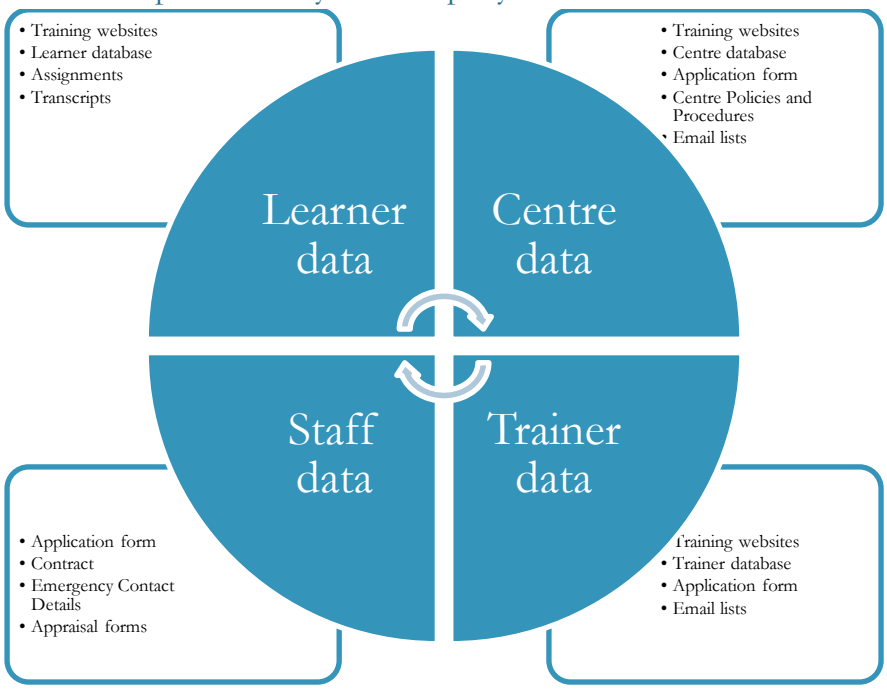
Other content will be added as risks are identified.

Gathering and checking information

Before personal information is collected, we will consider if it needs to be collected and for what lawful purpose. We will inform clients whose information is gathered. We will ensure that these records are kept up to date. Personal sensitive information will not be used apart from the exact purpose for which permission was given.

When people request information from our automated system, they receive an email to confirm they want to receive information from us, which is logged on our system. People contacting us by email or phone will be giving implied consent to be contacted in relation to their enquiry. Before receiving other marketing communications, their permission will be sought.

Personal data held and processed by the company



Data Storage

The company operates predominantly online, consisting of:

- Main website
- Training websites – a secure registration and resource portal
- Facebook groups – private support groups for attendees of courses and also trainers to enable them to seek support from peers

All online sites are stored and backed up on EU based servers.

The company uses Microsoft Office 365 for email and data files are stored locally on 2 computers and backed up to an off-site backup system. This enables the company to be able to guarantee data access

from one of the three storage points at any time. Accounts are secured with a password that includes numerals, alphabetic characters and symbols.

The digital company files are on a company system that requires the CEO to grant access to folders and files for individual members of staff. This means that they are unable to be accessed by anyone else. Personal data is not to be stored on removable devices without a specific agreement in place with the data protection officer.

Physical paperwork is minimised and the use of digital files is encouraged. Physical paperwork is stored in a locked filing cabinet within our coded access storage facility. This can only be accessed with the approval of the CEO and key fob access is required to the building, plus code for the storage room and key for the filing cabinet.

Staff who are working at home are expected to use online versions of files and save documents containing personal data online using the OneDrive access. They are permitted to temporarily download files to a password protected computer in order to work on them, but then must upload them and delete the downloaded version.

Data relating to individuals is normally kept for seven years (or until their 25th birthday), before being destroyed permanently by shredding or permanent deletion for digital files. There may be exceptions to this, for example, where we need to keep data relating to the award of qualifications.

Data access

Only authorised persons are allowed to access personal data. The company uses Microsoft OneDrive to store the majority of our data (explained above). Access privileges are authorised on a per user basis by the CEO and users are verified members of staff (i.e. their identity has been confirmed during their recruitment process).

Data sharing

For regulated qualifications, data is shared with both the awarding body and in England, the Education Skills and Funding Agency in order to administer the provision and assessment of the qualification.

For funded training, data is also shared with the funding bodies in order to be able to evidence and claim funding.

System assurance and monitoring

Data usage and suspicious activity are automatically monitored within Microsoft Office 365. The software contains built in protection malicious software, such as malware, in addition all devices accessing company data are protected by anti-virus/malware software.

Suspicious activity on user's accounts will automatically suspend users to protect data. Warnings and events are logged and investigated and actioned within 12 hours of being flagged up.

Risk management

A risk assessment of data and IT has been undertaken and is reviewed every 12 months, or more frequently if a threat is identified. This covers risks of malware, staff mistakes and criminal activity. This risk assessment and the annual review is approved by the Director.

Staff Responsibilities

All staff who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Staff will receive data protection training as part of their induction and receive updates every 12 months, or more frequently if a change, event or threat occurs.

Breach of this policy or unauthorised disclosure may result in disciplinary or legal action being taken.

Data Processing

To meet our responsibilities all staff will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

Computer and Network security

All staff are required to use password protected devices that are protected from viruses and malware, to access their Microsoft Office 365 accounts, including if they are home or mobile working.

Unsecured or public WiFi networks are not to be used (i.e. a WiFi network must be secured and accessed with a password). We do not have a network and so we there are no separate arrangements in place for network security.

Data transmission

Staff should ensure that personal data is transmitted using secure methods, such as direct email, Egress secure emails, sharing OneDrive direct links or secure file sharing software, such as Dropbox.

Data breaches

The company keeps data secure and monitors routinely for data breaches. In the event of a data breach that results in a high risk to the rights and freedoms of Individuals, the company will report the breach to the ICO within 72 hours (ideally within 24 hours). They will also inform the Individuals affected.

If a member of staff identifies a possible data breach in progress, they are required to act to stop the breach if possible, for example turning off the device where the breach is occurring, or calling the police in the event of intruders.

At the earliest opportunity the Data Protection Officer should be contacted by phone on 07938 329314. They will:

- attempt to contain the breach;
- attempt to recover, rectify or delete the data;
- record details of the breach, including the amount and type of data;
- notify the ICO;
- notify data subjects affected;
- notify other affected parties;
- take steps to prevent future breaches.

Staff duties

Staff working for the company are required to:

- Comply with this and the Staff IT User Agreement
- Consider the purpose of personal data and whether it needs to be collected.
- Ensure minimal personal data is stored appropriately using the company's IT system.
- Ensure that personal data is not shared unnecessarily.
- Refer to this policy or the Data Protection Officer if people request access to data.
- Use the company's OneDrive to store data.
- Not use unsecured or public WiFi.
- Not look at documents containing personal data where they can be overlooked (e.g. in public places).
- Ensure personal data that is being shared (for example to an awarding body) is transmitted in an appropriately secure method.
- Respond to data breaches immediately.
- Report any concerns to the Data Protection Officer.

Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to Richard Curtis, The Root Of It, 3 Merridale Road, Southampton, SO19 7AB.

Queries about handling personal information will be dealt with swiftly and politely. The company have the right to refuse or charge for requests that are manifestly unfounded or excessive. If a request is refused we will inform the Individual of the reason within 30 days, the Individual retains the right to complain to the ICO.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 30 days required by the GDPR from receiving the written request and relevant fee.

Right to be forgotten

Anyone whose data we hold has a right to be forgotten. Individuals seeking to use their Right to be Forgotten, should email info@rootofit.com with a form of ID or their Qualification Transcript to allow our staff to verify their identity. Once this is confirmed our staff will remove the records held on our online resource site(s) and email systems within 14 days. Due to the nature of our work, we are unable to remove the details of an individual from our training records.

Review

This policy will be reviewed biannually by the CEO.

September 2023