1. Overview

Norvic Training (UK) Ltd needs to gather and use certain information about individuals in the course of its ordinary operating activities. These include customers, suppliers, employees and any other people the organisation has a relationship with or may need to contact.
This policy describes how personal data is collected, stored and processed in order to meet the company's data protection standards and to be compliant with all relevant legislation.

This data protection policy ensures Norvic Training (UK) Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of all stakeholders
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach
- Only collects and holds data where there is a legitimate and necessary reason in order to achieve our business objectives.

Data Protection Law

Norvic Training (UK) Ltd regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. We will ensure that we treat personal information lawfully and correctly.

To this end Norvic Training (UK) Ltd fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act 1998 and the General Data Protection Regulations (GDPR).

We are committed to:

- ensuring that we comply with the eight data protection principles, as listed below
- ensuring that data is collected and used fairly and lawfully
- processing personal data only in order to meet our operational needs or fulfil legal requirements
- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data

- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- ensuring that a nominated Data Protection Officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- ensuring that all staff are made aware of good practice in data protection
- providing adequate training for all staff responsible for personal data
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines within the organisation

Data Protection Principles

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained for one or more specified and lawful purposes, and not further processed in any way that is incompatible with the original purpose
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose for which it is being used
- Personal data shall be processed in line with an individual's rights
- Personal data shall be kept secure with appropriate technical and organisational measures taken to protect the information
- Personal data shall not be transferred outside the European Economic Area (the European Union member states plus Norway, Iceland and Liechtenstein) unless there is adequate protection for the personal information being transferred

Individuals' Rights

- The right to be informed
- The right of access

- The right to rectification
- The right to be forgotten
- 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.

2. Policy Scope

This policy applies to all staff and all contractors, suppliers and other people working on behalf of Norvic Training (UK) Ltd.

It applies to all data that the company holds relating to identifiable individuals.

This policy helps to protect Norvic Training (UK) ltd from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

3. Responsibilities

Everyone who works for or with Norvic Training (UK) Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Everyone that handles personal data must ensure it is handled and processed in line with this policy and data protection principles.

However, the **Data Protection Officer** is responsible for:

- Reviewing all data protection procedures and related policies, in line with an agreed schedule – see point 12.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.

- Providing guidance on handling requests from individuals to see the data Norvic Training (UK) Ltd holds on them (Subject Access Requests).
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The **IT systems Manager** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data.

The **Development Manager** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Sharing data protection policy with current/prospective customers.

4. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Norvic Training (UK) Ltd will provide training to all employees to help them understand their responsibilities when handling data.
- Strong passwords must be used and they should never be shared.
- Employees should take reasonable care not to disclose personal data to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be archived (see point 5 for details).

- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

5. Data Storage

These rules describe how and where data should be stored safely. Questions regarding storing data safely can be directed to the Data Protection Officer.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly, in line with company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.
- When data is found to be out of date or no longer required it should be archived after which time it should be deleted.
- When an individual exercises their right to be forgotten, their personal data must be moved to the suppression list where it is held for three years before being either moved to the archive or deleted – depending on which route is appropriate.

- The legitimate interest document details current retention periods for the data held by Norvic Training.
- When employees have a legitimate reason to retain an email containing personal data, it should be held for a maximum of one year before being archived. Any email that does not need to be retained should be deleted.

6. Data Use

Personal data is of no value to Norvic Training (UK) Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared unless there is a legitimate business reason to do so.
- Employees should not save copies of personal data to their own computers/ mobile devices. Always access and update the central copy of any data.

Norvic Training does share personal information with the following third parties:

- Course information, including delegate name, is shared when required with course accrediting bodies for certification purposes – see legitimate interest document for current accrediting bodies used by Norvic.
- Email addresses are shared when, permission is specifically obtained, with our email messenger partner for the purposes of marketing – see legitimate interest document for current messenger partner.

7. Data Accuracy

The law requires Norvic Training (UK) Ltd to take reasonable steps to ensure that data is kept accurate and up to date. It is the responsibility of all employees who work with the data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take very opportunity to ensure data is updated. For instance, by confirming customer's details when they call.

- Norvic Training (UK) Ltd will make it easy for data subjects to update the information held about them for instance via the website.
- It is the Development Manager's responsibility to ensure marketing databases are checked against industry suppression files very six months.

8. Information we Hold

We conduct a legitimate interest assessment (LIA) for all personal data we collect – see separate LIA document (LIA001) for all details. This covers what information we can collect, why we collect it, who has access to it and how it is safely stored.

9. Communicating Privacy Information

Norvic Training (UK) Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights.

To these ends, the company has a privacy notice and consent form as follows:

Privacy notice

PRIVACY NOTICE
"At Norvic Training (UK) Ltd we use your contact details to remind you of when refresher/requalification training may be due. We also use it to tell you about relevant upcoming training courses and special offers. We will not without your express permission pass on your details to third parties for the purposes of direct marketing. You can withdraw consent to be contacted in this manner at anytime by contacting us in writing, via email or on the phone. A full copy of Norvic's Privacy Policy can be found **here** (hyperlink)."

10. Subject Access Requests (SAR)

All individuals who are the subject of personal data held by Norvic training (UK) Ltd are entitled to:

- Ask what information the company holds about them and why.

- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. There will be no charge for these requests. We will comply with a request within 30 days. If we refuse to comply we will tell the individual why and that they have the right to complain to a supervisory authority and for a judicial remedy. We must give them this information as soon as possible and within one month at the latest.

See attached Subject Access Request Checklist for a list of factors to consider before responding to a request. If staff members are unsure how to handle an SAR they should ask the Data Protection Officer for guidance.

11. Data Protection and Data Protection Impact Assessments (DPIA)

A DIPA 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.

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

13. Review Periods

This policy is to be reviewed every year.