Information Management And Privacy Policy

Jill Webb Training (JWT) is committed to the principles of Information Governance and Compliance with the General Data Protection Regulations (2018).

The principles of information governance are concerned with the management of information in an organisation. Information governance balances the use and security of information. It helps with legal compliance and operational transparency. An organisation can establish a framework for those working on behalf of the company to handle information through their information governance policies and procedures.

Information governance incorporates records management, information security and protection, risk management, privacy, data storage and archiving and knowledge management.

For JWT, this means that we make every effort to rigorously adhere with the requirements of the UK General Data Protection Regulations (GDPR) and UK Data Protection Law.

The aim of this Policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections. This is not only to ensure compliance with the GDPR and the Data Protection Act 2018 but also to provide proof of compliance.

As at August 2025, it is important to note that changes to the law have been agreed. The UK's data protection landscape is evolving with the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on June 19, 2025. This Act introduces changes to existing data protection laws, aiming to simplify rules for organisations, foster innovation and enhance law enforcement's ability to tackle crime while maintaining high data protection standards. As this law is implemented, this Policy will be kept under review.

Anyone working on behalf of JWT is required to comply with the terms of this Policy.

1. **What is GDPR?**

   The GDPR is the European data protection framework. GDPR requires any business that processes data belonging to UK citizens to protect it and not misuse it. As a responsible business, JWT aims to robustly implement the requirements of the UK GDPR. Part of meeting the obligation of meeting the obligations of UK GDPR is the production and implementation of this Policy. In addition, as required by these regulations, JWT is registered with the Information Commissioners Office https://ico.org.uk/ (Registration reference ZA760121)

JWT is committed to the rules of data protection and abiding by seven data protection principles. These are the principles that must be satisfied when obtaining, handling, processing, moving and the storage of personal data.

- Data must be obtained and processed fairly, lawfully and with transparency
- Data must be obtained for a specified, explicit and lawful purpose
- Data must be adequate, relevant and not excessive for its collection purpose ("data minimisation")
- Data must be accurate and kept up to date
- Data must not be kept for longer than is necessary for its purpose
- Data must be processed in accordance with the Data Subject's rights
- Data must be kept safe from unauthorised access, accidental loss or destruction ("integrity and confidentiality")

JWT does not collect any data on children aged under 16.

2. **How Does it Affect JWT?**
The GDPR is based on the core principles of data protection. In adhering to these principles JWT is committed to:

- collect no more data than is necessary from an individual for the purpose for which it will be used
- obtain personal data fairly from the individual by giving them notice of the collection and its specific purpose
- retain the data for no longer than is necessary for that specified purpose
- keep data safe and secure; and
- provide an individual with a copy of his or her personal data if they request it

3. **What Does This Mean in Practice For Clients Who Work With JWT?**
   - We will only ask for the relevant data required to run a course
   - This data will then be processed in accordance with the law
   - This data will be kept safe
   - This data will be destroyed when it is no longer needed. Details of the data retention schedule are shown in the Records Retention Policy
   - At any time, you can request that we destroy any data held on you. We would make you aware if destroying this data could have a detrimental effect on you, for example the inability to send out a certificate following a course
   - If we hold your details, we will contact you three or four times a year with information on forthcoming training opportunities. You can opt out at any time. Any marketing campaign follows the good practice guidance issued by the Information Commissioners Office
   - Emails containing factual information needed to access a course are, in law, 'service messages' and are exempt from this policy and GDPR legislation. We also retain the right to contact you if you owe JWT money
   - Very occasionally, we may need to pass your information onto someone else for your own welfare. For example, if you are taken ill on a course, or disclose something which makes us concerned that you are at risk or pose a risk to others. When we can, we will advise you that we need to do this

4. Privacy Statement

The principles of this policy are embedded in the following Privacy Statement:

Jill Webb Training is committed to protecting your personal data and privacy. We recognise that ensuring the accuracy and security of your personal data is essential to retaining your confidence and trust. The information you provide to us will only be used for the purposes that you provide it and will never be used for third party marketing. Full details of how we manage any information we hold about you can be found in the Jill Webb Training Information Management and Privacy Policy.

When we collect your personal data we will normally tell you:

- what your information will be used for
- who it may be shared with
- where you have a choice about your data we will ask for your consent to use it

5. Your Rights Under the GDPR - Data Subjects Rights

Under the GDPR individuals have rights Associated with their data, described below:

- 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
- Rights in relation to automated decision making and profiling

6. How do we Store Your information?

- Information is stored electronically on a passworded computer. The backup system is by use of an external hard drive which is stored securely
- All computer systems are virus checked on an on-going basis
- Some information pertaining to accredited courses is kept on the shared Google Drive for JWT. This data is subject to the same rigorous controls as all other data held by JWT. Access to the Google Drive is by password and is limited to personnel who have a reason to need to use the drive. Please be aware that Google may hold this information outside the EU
- Occasionally we have to hold data in hard copy, for example, if you have completed a registration form, this is held until it is transferred to electronic storage. Care is taken at all times to keep this as securely as possible. Hard copy records are destroyed by shredding, once they have been transferred to electronic storage in line with the permissions given by you
- Course registrations (which includes, name, address, contact details, ethnicity, signature) are removed from sight and access of other course learners immediately after completion
- Data is not disclosed or shared verbally or in writing to any unauthorised party
- If you visit our website we only collect your information with your specific consent, our company policy is to not take any action with IP addresses
- The secure service Mailchimp is used to manage our termly mailings. All protocols linked to this software are followed, and in line with best practice, individuals may unsubscribe at any time

7. Specific Data Protection Procedures For Those Undertaking Any ITC qualifications

In addition to the processes set out in sections 1 - 6, if you are undertaking an ITC qualification, JWT, as an approved ITC training centre, must collect and process information as required by ITC First awarding body and its regulators. JWT is therefore considered the Data Processor and its course learners and employees the Data Subjects.

JWT acts on behalf of ITC First, by gathering and submitting learner data securely via the ITC website and/or registered post. JWT has a legally binding Centre Agreement, which confirms that JWT publishes and implement a Data Protection Policy (this document).

JWT collects data as part of the booking and registration process required for qualification delivery. JWT collects and retains data as part of its administrative tasks.

When individuals provide their data to JWT, the data is submitted to ITC First and is used to:

- Attribute qualification credit to learners
- Produce commemorative certificates
- Produce CPD certificates
- Receive information pertinent to qualifications
- Enable ITC to contact you at your request (depending on when your data is provided and in which specific context or interaction with ITC First)
- Monitor ITC First qualifications to ensure equality and inclusivity

Learners' data will only be used for the legitimate purposes described above. Any changes to the ways in which learner data is used will be communicated to those individuals affected.

8. What Happens to Information I Provide?

JWT will download course learner data to their part of the ITC website and promptly submit all documentation to ITC First. Data submitted will only be viewable via individual unique user log on and password of JWT and ITC First.

JWT will not share their log on and passwords with any unauthorised individuals or companies.

9. What do we do if There is a Data Breach?

Jill Webb Training is registered with the Information Commissioners Office, and full details of this can be found here http://www.jillwebbtraining.co.uk

If security is breached, we will report this to the Information Commissioners Office within 48 hours.

We will inform clients as soon as possible about what has happened and what steps we have taken to rectify the situation.

10. How do we Respond to Subject Access Requests?

We respond to subject access requests by following the most up to date guidance published by the Information Commissioners Office. Should any requests for data appear to vexatious, JWT will notify the Information Commissioners Office. (www.ico.org.uk).

Any hard copy data will be destroyed in a confidential manner ie shredding of paper documents. Electronic records will be disposed of by deletion/psuedonymisation of digital records from computer systems.

JWT will ensure it does not retain data longer than is required for the purpose of the qualification as outlined in the Records Retention Policy.

This Policy will be reviewed every three years or earlier if a change in legislation, working practices or feedback from clients or partners necessitates.

This Policy was reviewed and updated in August 2025..