



Westwood Training and Consultancy

Data Protection Policy

Purpose

To make clear WTC's commitment to data protection. This policy links directly WTC's Privacy notice.

Policy Statement

We hold personal data on our employees, customers, clients and other associates of the business. We are committed to the principles of Data Protection legislation and this policy sets out our obligations and the requirements for collecting, storing and retrieving student/employee and service user records.

Westwood Training and Consultancy work will sometimes bring it into contact with confidential information. We will respect the privacy of staff, our learners and contractors. We aim to ensure that all learners can share their information in the confidence. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act and the Human Rights Act.

Scope

This policy statement covers all learners, staff, sub-contractors, volunteers, employers, partners and learners of the Centre. It also includes visitors, contractors and suppliers.

Data protection principles

The 1998 Act lists eight data protection principles relating to the processing of personal data held on computer systems and manual (paper) filing systems which are structured by reference to individuals.

Records kept on personal files can be processed only if specific conditions are met. These conditions include:

- the data must have been obtained fairly and lawfully;
- the processing is necessary for the performance of a contract with the individual;
- the data must be adequate, relevant and not excessive in relation to the purpose or purposes for which it is kept;



Westwood Training and Consultancy

- the data must be accurate and, where necessary, kept up to date;
- the data must not be kept for longer than is absolutely necessary;
- the data must be held in compliance with a learners/employee's rights of access to personal data, must not be processed in a way calculated (or likely) to cause damage or distress to a learner/employee, and must be corrected, erased or destroyed if inaccurate or no longer relevant;
- the data must be protected (by the best available means) against unauthorised access or disclosure and against accidental loss, damage or destruction; and must be treated as confidential by the staff to whom they are entrusted; and
- the data must not be transferred to any country or territory outside the European Economic Area (EEA) whose data protection laws or codes are non-existent or less than adequate – unless the employee agrees otherwise or the transfer is necessary for employment purposes (e.g. a proposed transfer or secondment overseas).

WTC's Obligations

WTC holds personal data about staff and learners. We need to process your personal data to carry out our legal duties under the employment and learner contracts.

The publishing of information such as an annual report, marketing material, etc. which contains employee / learners information is not prohibited, but the following guidelines should be followed:

Information about employees should only be published where:

- there is a legal obligation to do so
- the information is clearly not intrusive,
- the individual has consented to the disclosure,
- the information is in such a form that it does not identify individuals.

Where the employee / learner gives their consent, they should be made aware of the extent of information that will be published, how it will be published and the implications of this.

Under Data Protection legislation the 'reason' for sickness absence is classified as 'sensitive personal data' and as such must not be disclosed without the express consent of the individual.

As a consequence, the reason for illness will only be disclosed to the staff's line manager or the learners tutor. There should be no discussion or disclosure of the reason for sickness with any other person.



Westwood Training and Consultancy

Anyone whose personal data is being processed by WTC has certain rights in relation to their personal data. In practice, what this means is that individuals have the right, on written request and within a month, to:

- be told what personal data is being processed, why it is being processed, where it came from and to whom it may be disclosed
- access that data in an intelligible form
- ask to rectify the data if inaccurate
- ask for the data to be erased
- restrict processing
- data portability (in certain circumstances); and
- not to be subject to automated decision-making, for example in recruitment selection

Employee Obligations

All employees are required to take practical steps to comply with the principles, including keeping a clear desk outside working hours, ensuring personal data is never left visible or unattended on a desk, photocopier or computer screen.

You should never disclose personal information about another member of staff, a customer, supplier or client.

During the course of your work, you are likely to have access to information which is private or confidential to the Company, fellow or former employees, clients, customers or suppliers. You have a responsibility for the preservation of the confidentiality and integrity of information used during the course of your work.

If, as part of your role, you collect personal information about employees or other people such as clients, suppliers or colleagues, you must comply with this policy including the eight data protection principles.

You must also comply with the following guidelines at all times:

- Do not disclose confidential personal information to anyone except the data subject, unless the data subject has given their explicit prior written consent to this
- Ensure you verify the identity of the individual and the legitimacy of the request before releasing any personal information
- If you receive a request for personal information about another employee, you should forward this to Liz Barclay who is responsible for dealing with such requests
- Ensure any personal data you hold is kept securely and is not seen by unauthorised persons



Westwood Training and Consultancy

- Ensure that, when working on personal information as part of your job duties when away from your workplace, you continue to observe the terms of this policy, in particular in relation to data security
- Ensure that hard copy personal information is disposed of securely
- Take practical steps to support the adherence to the principles, for example keeping passwords separately from laptops and phones, using a strong password and not sharing your password with others

Remember that compliance is your personal responsibility

Please note that failure to follow the above obligations or comply with the Data Protection principles may be considered a disciplinary matter.

Sensitive data

Generally, where data relating to a student/employee/service user are of a sensitive nature, explicit consent must be obtained from the employee/service user to process the data and hold them on the individual's personal file. Sensitive data consist of information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious or other beliefs;
- physical or mental health;
- sex life or sexual orientation; or
- criminal convictions, proceedings or alleged activities.

Access to personal data

Learners and employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within 40 days.

Should a learner or employee request access to their personal data, the request must be addressed in writing to the relevant line manager. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.

In the event of a disagreement between an employee/ learner and the WTC regarding personal data, the matter should be taken up under the WTC complaints and appeals policy.



Westwood Training and Consultancy

Where students/employees make requests for access to their personal data which are granted, a fee of £10.00 will be charged which must be paid to the WTC before a copy of the personal data will be provided.

The right of learners/employees to see information held about them is extended to information held in paper record-keeping systems as well as computerised systems.

There are some exemptions; for example, learners/employees will not be able to see employment references about them supplied in confidence, nor will people involved in negotiations with the data controller be able to see information about the data controller's intentions in relation to those negotiations.

Learner/Employee data cannot be used for direct marketing (including fundraising) if the data subject objects. Approval to use student/employee data for marketing purposes must be sought from the Director of Communications.

Associated Policies and Procedures:

- Equal opportunities and Diversity Policy
- Staffing and Employment Policy
- Health and safety policy
- Learner recruitment policy
- Staff recruitment policy
- Privacy Notice
- Induction Policy

Review

The policy will be reviewed in September 2022

We will review this policy and its associated procedures annually as part of our self-evaluation arrangements and/or in response to customer, or regulatory feedback and any trends that may emerge in the types of queries we may have received.

Further information or queries For further information, or in the case of any queries over this policy or a particular matter of data protection, please consult the Data Controller.

Legal Framework

Data Protection Act 1998 (<http://www.legislation.gov.uk/ukpga/1998/29/contents>)

Freedom of Information Act 2000

Human Rights Act 1999

Policy and Procedures

January 2021, reviewed September 2024



Westwood Training and Consultancy

The Children Act 2004, 2006 (Every Child Matters)