2021

Confidentiality Policy

WEBS Training Limited
The Poplars,
Nottingham
NG9 2PD
0115 967 7771

Confidentiality Policy

Date: 2 February 2021

Purpose of Policy: Sets out the arrangements for managing confidentiality within WEBS.

Approved by: Nick Crowther (Board of Directors)

Responsibility for Updates: Lorraine Jameson (Head of Business & QA)

Policy applies to: WEBS employees

Version no: 5

Proposed Date of Review: February 2022

Version History			
Version	**Date**	**Detail**	**Author**
1	26.02.14	Refreshed – v1 draft	Sammy Jones
2	13/06/17	Review and Update	Sammy Jones
3	04/09/18	Review and Update	Sammy Jones
4	13/11/19	Review	Sammy Jones
4.1	13/01/20	Minor updates	Lorraine Jameson
5	02/02/21	Review & updates	Lorraine Jameson

Links and Dependencies

This policy is part of a suite of support policies aimed at supporting confidentiality of information.

- Complaints Policy
- Data Protection Policy & Procedures
- Disciplinary Policy
- E Safety Policy
- Information Security Policy
- Preventing Radicalization Policy
- Record Retention Policy
- Safeguarding Policy
- Staff Induction Procedures
- Subject Access Request Procedures
- Whistleblowing Policy

This is not an exhaustive list. A copy of a policy can be obtained on request or found in staff sharepoint.

Contents Page

General principles 4
Why information is held 5
Access to information 5
Storing information 5
Duty to disclose information 6
Disclosures 6
General Data Protection Regulations (GDPR)/Data Protection Act (DPA) 7
Breach of confidentiality 7
Whistleblowing 7
Monitoring and Review 7

Confidentiality Policy

General principles

WEBS recognises that colleagues (employees, volunteers, learners, board members & others who work within our organisation) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential.

This policy aims to give guidance but if in doubt, seek advice from the Head of Business & Quality Assurance.

Information received by WEBS as part of the services it provides, will be considered to be information for WEBS to share with colleagues and use to deliver its aims and objectives.

Staff should inform organisations or individuals why they are requesting information and explain the purpose of storing and using this information. Staff should ask permission to keep and use this information.

Staff are able to share information with other colleagues or the Head of Business & Quality Assurance in order to discuss issues and seek advice. Staff will not disclose to anyone, other than the Head of Business & Quality Assurance, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or a staff member, in the case of a WEBS employee.

Staff should avoid exchanging personal information or comments (gossip) about individuals with whom they have a professional relationship.

Staff should avoid talking about organisations or individuals in social settings.

There may be circumstance where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem.

If colleagues receive information from individuals outside WEBS regarding the conduct of a colleague or learner, then this should be dealt with sensitively. The appropriate staff member should tell the individual about the Complaints Procedure and advise them accordingly.

If employees are dissatisfied with the conduct of a colleague, and have sensitive information that could be evidenced through investigation, they should discuss it with the Head of Business & Quality Assurance under the Whistle Blowing Procedure. Any allegation, which is found to be malicious, or ill-founded, will be dealt with by WEBS action under the Disciplinary Procedure

Where there is a legal duty on WEBS to disclose information, the person that is affected will be informed that disclosure has or will be made.

Why information is held

Most information held by WEBS relates to individuals or service users, employees, board members, and volunteers (if appropriate).

Information is kept to enable WEBS Training Officers/Support staff to understand the needs of individuals or service users in order to deliver the most appropriate services.

Information about learners may be kept for the purposes of monitoring our equal opportunities policy and also for reporting back to the ESFA.

Access to information

Information is confidential to WEBS as an organisation and may be passed to colleagues, or board members to ensure the best quality service for all our users.

Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual who may request access to the information.

Colleagues will not withhold information from the Head of Business & Quality Assurance unless it is purely personal to them and not business related.

Employees/Learners may see WEBS records which relate to them or their organisation. The request must be in writing to the Head of Business & Quality Assurance giving 14 days' notice. The letter must be signed by the individual, or in the case of an organisation's records, by the Chair or Executive Officer or Manager.

Sensitive information will only be made available to the person or organisation named on the file.

Employees may see all of their personnel records by giving 14 days' notice in writing to the Head of Business & Quality Assurance.

When photocopying or working on confidential documents, employees must ensure they are not seen by people in passing. This also applies to information on computer screens.

Storing information

General non-confidential information about organisations is kept in unlocked filing cabinets that are available to all WEBS employees.

Information about learners and employers will be kept in lockable filing cabinets in a locked room.

Employees' personnel information will be kept in lockable filing cabinets and will only be accessible to the Head of Business & Quality Assurance, and Head of Programme Management.

Files or filing cabinet drawers bearing confidential information should be labelled ‘confidential’.

In an emergency situation, the senior managers may authorise access to files by other people.

Only data required for employment purposes i.e. lawfully will be collected and retained during the period of employment.

All confidential documentation or personal data must be shredded before putting in the recycling bins.

Duty to disclose information

WEBS have a legal duty to disclose some information including:

- Child abuse which will be reported to the Children’s Services / Social Services Department (refer to the Safeguarding Policy)

- Drug trafficking, money laundering, acts of terrorism or treason which will be disclosed to the police (refer to the Safeguarding Policy).

In addition a colleague believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the Designated Safeguarding Lead, where appropriate, who will report it to the appropriate authorities.

WEBS should inform the individuals concerned of this disclosure.

Disclosures

WEBS comply fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

WEBS will request pre-employment Disclosure and Barring Service (DBS) checks for new employees and volunteers whose posts involve contact with vulnerable children or adults, as specified by the Disclosure Guidance.

WEBS will clearly state the need for, and level of disclosure on the recruitment advert.

Disclosure information is always kept separately from an applicant’s personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

Documents will be kept for a year and then destroyed by secure means. Photocopies will not be kept. However, WEBS may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, and the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

General Data Protection Regulations (GDPR)/Data Protection Act (DPA)

Information about individuals, whether on computer or on paper falls within the scope of the GDPR/DPA and must comply with the data protection principles.

These are that personal data must be:

- Obtained and processed fairly and lawfully
- Held only for specified purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the Act
- Kept secure and protected
- Not transferred outside of Europe

WEBS will ensure that it conforms to all aspects of the GDPR/Data Protection Act. Please refer to WEBS Data Protection Policy for detailed information on how we will do this.

Breach of confidentiality

Employees/Board Members or other WEBS users who are dissatisfied with the conduct or actions of other colleagues or WEBS staff should raise this with the Head of Business & Quality Assurance using the grievance procedure, if necessary, and not discuss their dissatisfaction outside WEBS.

Employees accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

Whistleblowing

Any employees who have concerns about the use of WEBS funds, or any practice by any employee must comply with the requirements of the Whistle Blowing Policy.

Monitoring and Review

This policy will be reviewed at an appropriate time or when legislation dictates but not later than two years after ratification by the board of Directors.