Confidentiality Policy

Purpose

Our confidentiality company policy refers to the safety and disclosure of important information that the company holds. During everyday business, employees will unavoidably receive and handle personal and private information about clients, learners, employers, partners, stakeholders and the company. This policy is designed to set the rules that will protect this information from exposure.

Scope

This policy affects all employees and others that may have access to confidential information, such as services, suppliers, part time employees, substitute employees, board members, investors, contractors, volunteers, auditors, stakeholders etc.

Policy elements

Information that the company considers confidential and proprietary is undisclosed, valuable, expensive and/or easily replicated. More specifically, information that is classified as confidential includes:

- Customer lists (existing and prospective)
- Data of Customers including Learners/Employers/ Partners/Vendors/Stakeholders
- Trade secrets
- Private deals
- Unpublished financial information
- Processes, methods and know-how
- Patents or new technologies
- Pricing/marketing and other undisclosed strategies or tactics
- Unpublished goals, forecasts or initiatives that are marked as confidential
- Data entrusted to the company by external parties
- Documents, processes or other elements explicitly marked as confidential, or for which directors have in writing is confidential
- Any other knowledge acquired by employees during their employment

(This list is not exclusive, and employees must consult with leadership and management team should they have any questions on what constitutes personal, private and confidential information)
All these types of information must be protected for different reasons – some may be legally binding (e.g. sensitive data) and some constitute the backbone of the business and give it a competitive advantage (e.g. business processes).

The disclosure of some kinds of information may expose the company to increased risk such as specific trade secrets, while for others the result could be the loss of important partners, loss of reputation and/or non-compliance with data protection laws.

In the course of their employment, employees will have various levels of authorised access to confidential information so as to conduct their business. When they do so, the following rules strictly apply:

- No amount of information will be disseminated to anyone outside of the organisation.
- The disclosure of information inside the organisation will be limited to those with authorised access and legitimate reason to require that information.
- The information will not be used for the personal benefit or profit of the employee or any other except the company.
- The employee can only access only the amount and type of information required for the completion of their job responsibilities and no more.
- If working remotely, employees and everyone must ensure confidential information is dealt with in a way that is compliant with the data protection laws and that is handled through the use of TDM internal systems.
- When perusing or sharing information through electronic means, all precautionary safety measures must be in effect and the information security policies must be followed through also extra care when sharing information with external email addresses that are not in the TDM systems.
- If the staff member knows that the channel of sharing communication is not secure and where the data is confidential they must seek help from the IT team to secure documents and send following encryption processes.
- Confidential information must not be left unattended or unlocked.
- Unauthorised replication of information is prohibited.
- When no longer needed, all copies of confidential documents must be shredded, or securely disposed of, following the safe disposal of confidential information procedure.
- Upon separation of employment all confidential information must be returned or deleted from the employee's electronic devices.
- Employees must not store Confidential or Personal information belonging to TDM, TDM's clients, employers, learners and stakeholders in any personal device nor personal system.
- Where a learner has shared confidential information relating to their employment, the TDM coach must make an evaluation if this is a safeguarding or a welfare issue and signpost accordingly. If a safeguarding issue, the designated safeguarding Lead must be notified. However if a welfare issue coaches should encourage learners to communicate with the employer, since the sharing of this information with the employer will in most cases result in support for the learner to overcome barriers. Where the learner does not want to share information with the employer , the issue needs to be highlighted to the line manager.

The company will take measures to ensure that confidential information is well protected. Those measures include but are not limited to:

- Electronic information will be encrypted
- Databases will be protected with all available security measures

- Paper documents will be safely stored and locked to be accessed by authorised personnel only.
- Authorisation of access will be carefully controlled, usually by senior management.
- Employees may need to sign non-compete and/or non-disclosure agreements.

Confidential information as described above may occasionally have to be disclosed for legitimate reasons, e.g. upon request of a regulatory body or for business purposes. In such cases, a strict procedure must be followed that includes the explicit consent of parties involved (unless they are faced with criminal charges) and the disclosure of only relevant information and no more. See Appendix 1.

Disciplinary Consequences

The company places great importance in all its information security policies.. Any non-conformity will bring about disciplinary and, possibly, legal action. The company is prepared to terminate any employee who wilfully or regularly breaches the confidentiality guidelines for personal profit.

Serious offences such as theft of information, illegal disclosure of sensitive data etc. will be grounds for immediate for-cause dismissal and may also involve legal consequences. Any unintentional breach of this policy will be thoroughly investigated and will be dealt with appropriately depending on its magnitude and seriousness. This policy is binding even after separation of employment.

Appendix 1

Disclosure of Confidential information Procedure

If a regulatory body or TDM customer asks for disclosure of confidential information, the following strict procedure must be followed.

1. Check the identity of the request- Is it genuine?
2. Check the nature of the request – does it need this procedure?
3. Inform the leadership and management team of the request and seek for approval in writing. This must explain the case and reasons. Subject of letter must be “Request authorisation of confidential information”
4. Leadership and management team reviews the request and approves in writing, giving specific guidelines if necessary.
5. Confidential information is disclosed stating “Strictly Private and Confidential” as the first part of the disclosure.
6. Leadership and management team must work together with the information security officer in place.

Please also see:
Data protection policy

Versions

Issue No	Issue Date	Revision No	Revision Date	Section	Revision Details	Author
1	20/09/2016	0				
1	20/09/2016	1	21/06/2017	Page 2 Page 3	Top - Added additional information regarding confidential information Paragraph 2 – Add on to see Appendix 1 Added Appendix 1 - Procedure for Disclosure of Confidential Information	Elizabeth Kent Elizabeth Kent Elizabeth Kent
1	20/09/2016	2	16/01/2018	Page 1 Page 4	Added specific names for clients, customers: employers, learners Added to appendix: Top management must work in conjunction with Information Security Officer.	Elizabeth Kent
1	20/09/2016	3	21/11/2019	Page 2	Added clause when learners share data with coaches and employer to be informed best practice (if circumstances permit)	Elizabeth Kent
1	20/09/2016	4	21/11/2019	All	Updated information to reflect new position of business (Covid)	EK BP
1	''	5	11/11/2021		Reviewed all sections. Added auditors	EH, BP