Confidentiality policy

Version:	4
Policy Owner:	Alison Williams
Associated documents:	Non-Disclosure Agreement
Review date:	Dec 2024
Reviewed by:	Stephanie Jones
Agreed by:	Senior Leadership Team
Next review date:	Dec 2025
Summary of changes: Full rewrite to include explicit details around protecting information from assessments / EPA evidence.	

Contents

Purpose

This Confidentiality Policy explains the procedures for safeguarding the confidentiality of all sensitive information handled by Marshall Assessment (MA) in the context of End-Point Assessment (EPA) and the running of the organisation for the purpose of EPA delivery.

Marshall Assessment must ensure that all data, documents and communications are managed securely to maintain the integrity and confidentiality of the assessment process and to protect all parties.

This policy outlines how Marshall Assessment expects all staff, consultants and stakeholders to treat confidential information.

Staff, consultants and stakeholders may have access to information which:

- is sensitive customer data or commercially sensitive information through evidence provided in the assessment process.
- constitutes the backbone of our business, giving us a competitive advantage (e.g. internal business processes)
- is Marshall Assessment's intellectual property (assessment materials).

It ensures that all information obtained during the assessment process, whether relating to apprentices, employers, staff, or business operations, is treated with the utmost confidentiality, in line with relevant legal and regulatory requirements.

Scope

This policy applies to all employees of Marshall Assessment, but also including all members of the board, contractors and consultants, who may have access to confidential information. It covers all forms of information, including but not limited to verbal, written, electronic or digital data.

Definitions

Confidential Information: Any information that is not publicly available and which, if disclosed, could harm the interests of individuals, organisation's or the integrity of the EPA process.

For Marshall Assessment this includes, but is not limited to:

- Personal data - any information that relates to an identified or identifiable individual, including but not limited to names, contact details, and identification numbers
- Assessment results/ marking/ evidence/ IQA feedback
- Data relating to Marshall Assessment's customers/ employers /apprentices
- Assessment materials / question banks / test papers
- Sensitive data or commercially sensitive information entrusted to Marshall Assessment by external parties for the purpose of End-Point Assessment, for example, evidence received from apprentices in the way of reports /articles or portfolios.
- Unpublished financial information

Marshall Assessment consultants and staff may have various levels of authorised access to confidential information.

Legal Framework

This policy supports compliance with relevant legislation and regulations, including but not limited to:

- Data Protection Act 2018.
- UK General Data Protection Regulation (UK GDPR)

Responsibilities

- **Employees and Consultant Assessors**: Must adhere to this policy and take all reasonable steps to protect confidential information from unauthorised access or disclosure.

All individuals working for or on behalf of Marshall Assessment are responsible for maintaining the confidentiality of all information handled and accessed during their work. They must ensure information is only shared on a need-to-know basis (with consent of the individual) and for legitimate business purposes, and not kept for longer than required in line with Marshall Assessment's Data Protection Policy.

- **Management**: The Senior Leadership Team are responsible for ensuring that all personnel are aware of and comply with this policy, and for providing training on confidentiality and data protection in line with UK GDPR.

What Marshall Assessment staff and consultants must do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure they only view confidential information on secure devices
- Only disclose information to other employees when it's necessary and authorised
- Keep confidential documents stored within the allocated Marshall Assessment SharePoint folder or secure Information Management platform as appropriate.

What Marshall Assessment staff and consultants must NOT do

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of Marshall Assessment or beyond what is required for the purpose of the business activity
- Replicate confidential documents and files and store them on insecure devices

When employees stop working for our company, they are obliged to return any confidential files and delete them from their personal devices.

Confidentiality Measures

All employees and contractors / consultants will sign a non-disclosure agreement (NDA) at the point of recruitment / registration with Marshall Assessment.

- **Data Protection**: All personal data and confidential information must be stored securely, either physically or electronically, using appropriate measures such as password protection, encryption, and secure storage facilities in line with MA's processes and procedures.
- **Access Control**: Access to confidential information is restricted to authorised personnel only and based on the principle of "need to know." Access rights must be regularly reviewed and adjusted as necessary.

- **Document Handling**: Confidential documents must be handled with care, ensuring they are not left unattended or exposed to unauthorised individuals. Shredding (digital shredding where electronic) or secure disposal of physical documents is required when they are no longer needed.
- Measures are in place on our Information Management platform and SharePoint Site to ensure that confidential or sensitive information is accessed only by those personnel required to have access for the purpose of the EPA processes (assessment delivery, IQA, administration).
- IT systems in place to safeguard databases and information storing sites

Confidentiality in External Relationships

When dealing with third parties (including apprentices, employers, training providers and regulatory bodies), Marshall Assessment will ensure that any confidential information shared with or by these parties is protected under the existing non-disclosure agreement or is subject to additional confidentiality agreements or similar protective measures to safeguard its security and commercial sensitivity where required.

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. For example, if our regulatory body requests it as part of an investigation or external quality assurance.

In such cases, the Marshall Assessment staff involved should document their disclosure procedure and collect any required authorisations.

Data Breach Protocol

In the event of a data breach or suspected breach involving confidential information, the following steps must be taken:

1. **Immediate Notification**: Notify the Marshall Assessment Managing Director (MD)- if required the relevant authority will be notified.
2. **Assessment**: The MD and /or relevant authority will assess the breach, including its scope and impact.
3. **Containment**: Take appropriate steps to contain and mitigate the breach.
4. **Reporting**: Report the breach to any relevant regulatory body if required by law and notify affected individuals if necessary.
5. **Review**: Conduct a review to determine the cause of the breach and implement measures to prevent recurrence.

Employees who do not follow procedure and knowingly breach our confidentiality policy will face disciplinary and possibly legal action. See Malpractice and Maladministration policy for additional information regarding reporting and investigation procedure.

We will investigate any breach of this policy. We will terminate any employee who willfully breaches our confidentiality guidelines for personal profit. We may also issue sanctions for any unintentional breach of this policy depending on its frequency and seriousness. We will terminate the contract of employees who repeatedly disregard this policy, even when they do so unintentionally.

MA reserves the right to take legal action against individuals or entities that breach confidentiality agreements.

Training and Awareness

All personnel must receive regular training on confidentiality and data protection, including updates on relevant laws and regulations. The Organisation will provide resources and support to ensure ongoing awareness and compliance.

This policy is binding even after separation of employment.

Contact Information

For any questions or concerns regarding this Confidentiality Policy, please email: helpdesk@marshall-assessment.com

Review and Updates

This policy will be reviewed annually or as needed to ensure its effectiveness and compliance with applicable laws and regulations. Any changes to the policy will be communicated to all relevant parties.