Wonderment

Wonderment Information Security Policy

Overview

To protect client and company information from unauthorised access, disclosure, alteration or destruction.

Scope

This applies to all data, files and communications handled by Wonderment Creative Ltd, whether digital or physical.

Principles

1. Confidentiality – Client information is only accessed by those who need it.
2. Integrity – Data is kept accurate, consistent and secure from alteration.
3. Availability – Information is only accessible to authorised parties when required.

Key Practices

- Access Control: All devices are password-protected; sensitive files use encryption where possible.
- Data Handling: Client files are stored securely (cloud systems with encryption, e.g. Google Workspace/Dropbox Business).
- Sharing: Files are only shared via secure links, never open email attachments where possible.
- Physical Security: Devices are locked when unattended. No sensitive information left on desks.
- Backups: Regular cloud backups to prevent data loss.
- Email Security: Two-factor authentication enabled; vigilance against phishing emails.
- Software & Updates: Devices kept updated with the latest security patches and antivirus software.
- Third Parties: Any subcontractors or partners are required to follow equivalent security measures.
- Incident Response: In case of a suspected breach, the client will be notified immediately and corrective steps taken.

©Wonderment Creative Ltd 2025. - All rights reserved. Do not share, copy, reproduce or sell any part of this document unless you have written permission from Wonderment Creative Ltd.

Responsibilities

- All team members are responsible for safeguarding information.
- Leadership ensures policies are communicated and reviewed annually.

Review

This policy is reviewed annually or sooner if risks or technologies change.

©Wonderment Creative Ltd 2025. - All rights reserved. Do not share, copy, reproduce or sell any part of this document unless you have written permission from Wonderment Creative Ltd.