Information Security & Client Data Handling Policy

Business: MarketingSteve
ABN: 52719351544
Effective Date: October-2026
Last Reviewed: October-2026
Review Frequency: Annually or following material changes to business operations

1. Purpose

This policy establishes how MarketingSteve protects confidential information, personal information and business data accessed, received or created during its operations.

The objective is to maintain appropriate information security while supporting efficient, practical delivery of professional marketing services.

Security measures will be proportionate to the nature and sensitivity of the information handled, the risks involved and the resources reasonably available to the business.

2. Scope

This policy applies to:

- Information collected or maintained for the business's own operations.
- Client information accessed or handled in connection with professional engagements.
- Business-owned devices, cloud accounts, software and communication systems.
- Subcontractors or freelancers authorised to handle information on behalf of the business.

The sole trader is responsible for implementing this policy and reviewing its effectiveness.

3. Client Data Ownership and Responsibility

Client information remains the property or responsibility of the relevant client, subject to applicable legal rights and obligations.

Clients are responsible for ensuring that information provided to the business has been lawfully collected and may be disclosed or used for the agreed purposes.

The consultant will handle such information only as reasonably necessary to perform the agreed services and in accordance with applicable confidentiality, privacy and contractual obligations.

4. Data Minimisation

The business will avoid collecting, accessing, copying or retaining information that is not reasonably required for the services.

Where practicable:

- Aggregated or de-identified data will be preferred over identifiable personal information.
- Access to client systems will be preferred over exporting large datasets.
- Only information relevant to the agreed work will be downloaded.
- Duplicate files and unnecessary working copies will be minimised.

Sensitive information, including health records, identity documents, financial credentials and other high-risk personal information, must not be intentionally collected or processed unless reasonably necessary and expressly agreed with the client in writing.

Additional safeguards will be considered before accepting such information.

5. Client-Owned Systems

Where reasonably practicable, client information will remain within client-owned or client-controlled systems.

These may include:

- Customer relationship management platforms.
- Cloud document storage.
- Advertising and analytics accounts.
- Website content management systems.
- Email marketing and automation platforms.
- Project management and collaboration tools.

The consultant will use authorised access permissions and avoid unnecessary transfers of information outside those systems.

The client remains responsible for overall administration and security of its systems unless otherwise agreed.

The consultant remains responsible for using granted access appropriately and securely.

6. Storage on Business Devices and Accounts

The consultant may store working documents, project files, research, analysis, correspondence and other necessary information on business-controlled devices or cloud accounts.

Where client information is stored outside client-owned systems, the consultant will:

- Use reputable storage platforms with appropriate security capabilities.
- Maintain appropriate authentication and access controls.
- Limit stored information to what is reasonably necessary.
- Keep confidential client information separate from publicly accessible materials.
- Avoid sharing files through unsecured public links.
- Review and remove unnecessary copies when work is completed.

Confidential or sensitive files should not be stored in publicly accessible folders or transferred through services that do not provide appropriate safeguards.

7. Device and Account Security

Devices and accounts used for business activities must have reasonable security protections.

These include:

- Passwords or passphrases that are unique and appropriately strong.
- Multi-factor authentication wherever supported, particularly for email, banking, cloud storage and client systems.
- Automatic device locking and appropriate screen-lock settings.
- Regular operating system and software updates.
- Appropriate malware protection and firewall settings.
- Reasonable physical protection against theft, loss or unauthorised use.

Business devices should not be left accessible to unauthorised individuals.

8. Passwords and Access Permissions

Passwords, authentication codes and other credentials must be treated as confidential.

Where possible:

- Individual user accounts will be used instead of shared logins.
- Passwords will be managed through a reputable password manager.
- Client access will be restricted to the permissions reasonably necessary for the services.
- Administrative permissions will only be used where required.
- Access will be removed or relinquished when no longer necessary.

Credentials must not be disclosed to unauthorised individuals or entered into untrusted websites or applications.

9. Information Sharing and Transfer

Confidential information must only be shared with individuals who have a legitimate business need and appropriate authorisation.

Where practicable, the consultant will use client-approved collaboration systems, secure cloud sharing or other reasonably protected transfer methods.

Before sending confidential or personal information, reasonable steps must be taken to verify the recipient and ensure the information is appropriate for disclosure.

The consultant will avoid transmitting sensitive information through unsecured or unnecessarily exposed communication channels.

10. Artificial Intelligence and External Tools

Artificial intelligence-assisted tools may be used for research, analysis, strategy development, content preparation and other legitimate business activities.

However:

- Identifiable personal information, sensitive information and materially confidential client information must not be intentionally submitted to external generative AI services without appropriate written client authorisation and consideration of applicable legal and security requirements.
- Where possible, information should be anonymised, summarised or otherwise minimised before being entered into AI systems.
- AI tools must not be granted unnecessary access to client systems or databases.
- AI-assisted outputs must be independently reviewed before being relied upon or incorporated into client deliverables.

- Raw, unreviewed AI-generated outputs must not be delivered to clients as completed professional work.

The consultant remains responsible for the quality, accuracy and professional appropriateness of work delivered using AI-assisted technologies.

11. Subcontractors and Freelancers

Where subcontractors or freelancers are engaged, access to client information must be limited to what is reasonably necessary for their authorised work.

Before providing access to confidential information, the consultant must ensure appropriate confidentiality, information security and permitted-use obligations are in place.

Subcontractors must not independently disclose, retain or reuse client information outside their authorised responsibilities.

Their access must be removed when no longer required.

Any proposed subcontracting must also comply with the relevant client agreement, including any consent requirements.

12. Backups and Recovery

Important business records and working files will be backed up using suitable methods proportionate to the nature of the information and the potential impact of its loss.

Where practicable, backups will be maintained through reputable services with appropriate security protections.

The consultant will periodically confirm that important business information can be recovered.

The consultant is not responsible for maintaining independent backups of information retained in client-owned systems unless expressly agreed.

13. Information Retention and Disposal

Business and client information will be retained only for as long as reasonably necessary for legitimate operational purposes, contractual obligations, legal recordkeeping or the establishment or defence of legal claims.

Following completion or termination of an engagement:

- Client-owned deliverables and necessary information will be made available in accordance with the relevant agreement.
- Access to client-controlled systems will be relinquished or revoked.
- Unnecessary working copies and duplicate files will be securely deleted within a reasonable timeframe.
- Information required for legitimate recordkeeping may be retained under appropriate safeguards.

Information retained in routine system backups may remain until those backups are replaced or deleted through normal processes.

14. Security Incidents

Suspected or confirmed unauthorised access, data loss, account compromise or other material security incidents must be addressed promptly.

The consultant will follow the Data Breach & Incident Response Procedure and comply with applicable client notification and legal requirements.

15. Review and Continuous Improvement

Security practices will be reviewed at least annually and following material changes to technology, business operations, the nature of client information handled or identified security risks.

This policy will be updated where reasonably necessary to maintain appropriate protection.