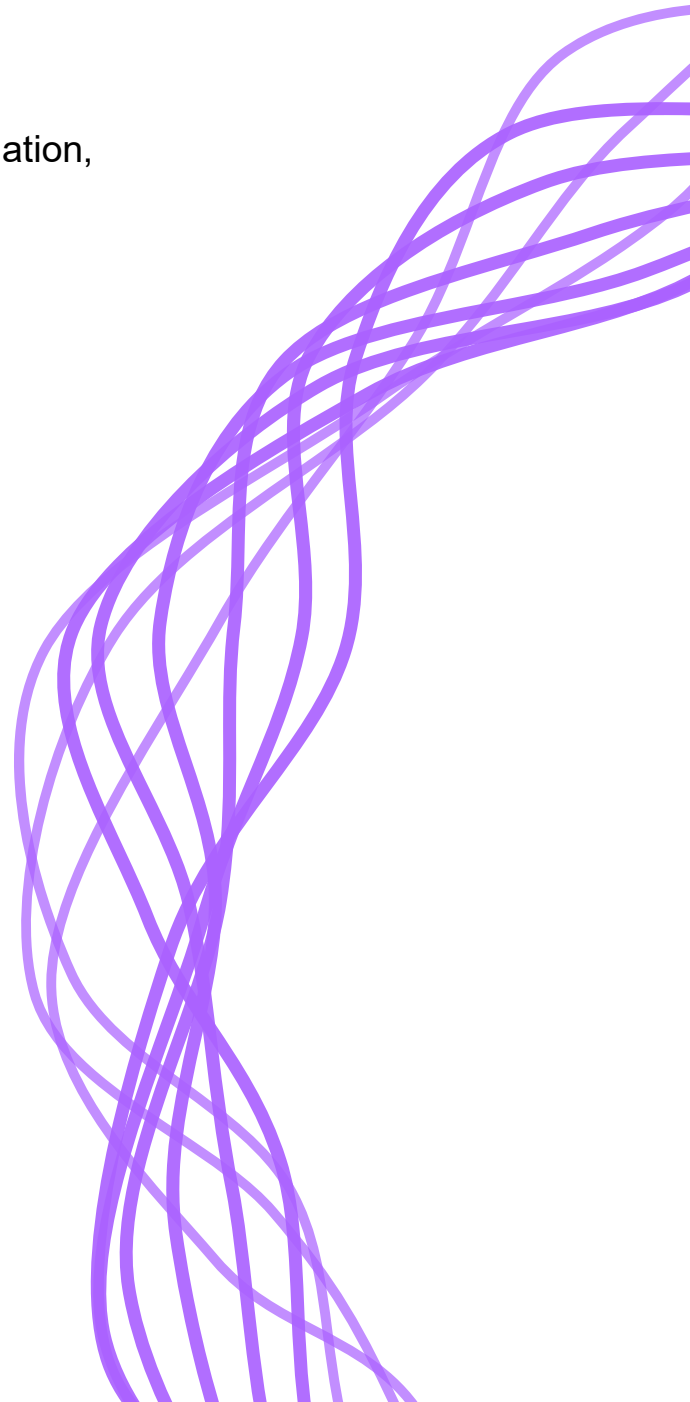
doublespark®
Internet Marketing

Doublespark Ltd Information Security Policy

Our approach to safeguarding client information, systems and digital services.



Doublespark Ltd
Company Policies

3 November 2026

doublespark®
Internet Marketing

Information Security Policy

Company Policy | Version 1.0

POLICY OWNER Gary Cottam, Managing Director	**APPROVED BY** Gary Cottam, Managing Director
EFFECTIVE DATE 3 November 2026	**NEXT REVIEW DATE** 3 November 2027
REVIEW FREQUENCY Annually	**DOCUMENT VERSION** 1.0

1. Our Commitment

Doublespark Ltd is committed to protecting the confidentiality, integrity and availability of information entrusted to us by clients, employees and business partners.

We recognise that effective information security is an essential part of providing reliable digital marketing, website development, hosting and consultancy services.

Our objective is to protect information against unauthorised access, accidental loss, disclosure, alteration and misuse through appropriate technical and organisational measures.

2. Access Control

Access to client information, systems and services must be restricted to authorised individuals with a legitimate business requirement.

We apply the following principles:

- User access is granted according to operational requirements.
- Administrative access is restricted to appropriate personnel.
- Strong authentication is required, with multi-factor authentication used for sensitive systems where supported.
- Access permissions are reviewed when responsibilities change and removed when no longer required.
- Passwords, API keys and other authentication credentials must be stored and handled securely.

3. Information Handling

Employees and contractors must handle confidential and personal information responsibly.

Information must only be accessed, used, retained or shared for authorised business purposes.

Appropriate security measures must be used when transferring or storing confidential information, taking account of its sensitivity.

4. Systems and Infrastructure

Doublespark Ltd is committed to maintaining appropriate security measures for the systems and infrastructure under its management.

These include, where applicable:

- Timely application of relevant security updates and patches.
- Appropriate firewall and access protection.
- Monitoring for security threats and suspicious activity.
- Backup and recovery arrangements appropriate to the services provided.
- Secure configuration and management of systems and software.
- Appropriate controls over third-party service providers.

5. Security Incidents

Suspected information security incidents must be reported promptly to the responsible Company Director.

Incidents will be assessed and managed according to their nature and potential impact.

Where necessary, affected clients, relevant authorities or other parties will be notified in accordance with applicable legal and contractual requirements.

6. Employee and Contractor Responsibilities

Everyone granted access to Doublespark or client information must comply with applicable security requirements and protect confidential information against unauthorised access or disclosure.

7. Compliance and Review

Doublespark Ltd aims to comply with applicable UK data protection legislation, including the UK GDPR and Data Protection Act 2018.

This policy will be reviewed annually and following significant changes to our operations, technology or security risks.