

Data Protection, Confidentiality and Responsible AI Policy

GreenSpark will handle personal data, client information and confidential material lawfully, securely and only for legitimate purposes. AI tools may support productivity where approved, but must not compromise confidentiality, privacy, accuracy, intellectual property or professional judgement.

Status: Final — Approved and Published **Version:** 1.0

Approved: 1 July 2026 **Published:** 1 July 2026

Policy owner: GreenSpark Consulting — Management **Next review:** 1 July 2027

Policy statement

GreenSpark will handle personal data, client information and confidential material lawfully, securely and only for legitimate purposes. AI tools may support productivity where approved, but must not compromise confidentiality, privacy, accuracy, intellectual property or professional judgement.

1. Scope

Applies to all covered persons using company or client data, devices, systems, AI tools, email, collaboration platforms and physical records.

2. Data protection and confidentiality

Comply with applicable data protection law, confidentiality obligations, contractual controls and information-security requirements.

- Collect and use only information necessary for a defined purpose and retain it only for an appropriate period.
- Use approved accounts, access controls, strong authentication and secure sharing methods. Check recipient details before sending sensitive information.
- Respect client confidentiality and third-party intellectual property. Share information only with authorised recipients and on an appropriate basis.

3. Responsible use of AI

- Do not enter personal data, client-confidential material, credentials, commercially sensitive information or restricted project information into an AI service unless the tool and use have been approved for that data.
- Verify AI-generated facts, calculations, citations and recommendations against reliable sources before relying on them.

Human review is required for material AI-generated outputs used in client advice, commercial decisions, compliance assessments or external communications.

- Do not use AI to fabricate evidence, misrepresent expertise, make unsupported claims or produce discriminatory or unlawful outcomes.
- Disclose AI use to clients where contract, law, professional standards or the nature of the work requires it.
- Do not make solely automated decisions with legal or similarly significant effects on individuals without appropriate legal review and safeguards.

4. Security incidents

- Report suspected data loss, unauthorised access, misdirected information or unsafe AI use promptly to the designated data/security lead.

Contain the incident where safe to do so, preserve relevant evidence and avoid deleting records needed for investigation.

- Assess notification duties and contractual obligations, including whether a regulator, affected individual or client must be informed. Record remedial actions and lessons learned.

5. Responsibilities and review

Management approves systems and defines acceptable use. Each user protects credentials, follows data-handling rules and checks AI outputs. The designated lead coordinates incident response, access reviews and retention practices.

- Maintain an inventory of systems and AI tools, access approvals, relevant processing records, training, data-sharing terms, retention schedules and incident logs.

Review annually and after significant changes in technology, services or law.

Related guidance

Complete any required privacy notices, data-processing agreements, international transfer safeguards and impact assessments before relevant processing begins.

Approval and document control

This is the published version 1.0 of this policy, with approval and publication dates recorded as 1 July 2026. It forms part of the GreenSpark Consulting — Governance, Integrity & Responsible Business framework and should be read with other relevant policies and applicable law.

Approved status: Approved **Effective date:** 1 July 2026 **Review date:** 1 July 2027