

Document reference: G-05 | Region: Global | Version: [TBD] | Effective date: [TBD]

WORKING DRAFT - PUBLICATION CONTROL: This document is drafted for the RedTree launch. Do not publish until the Global Compliance Matrix confirms the related launch implementation. Any text marked 'TBD BEFORE PUBLICATION' must be resolved and removed before release.

1. Principle

RedTree is intended to help users capture, organise, store, search, synchronise and analyse lawful information and content. Users remain responsible for how they use the service.

2. Prohibited uses

- Committing, facilitating or concealing unlawful activity.
- Accessing accounts, systems or data without authorisation.
- Introducing malware, exploiting vulnerabilities or deliberately disrupting RedTree or third-party systems.
- Circumventing subscriptions, entitlements, security controls or usage limits fraudulently.
- Using RedTree infrastructure for attacks, intrusion, fraud, spam or abusive automated activity.
- Infringing intellectual-property, privacy, confidentiality or other rights of third parties.
- Storing or processing content where possession or processing of that content is itself unlawful.

3. Third-party data and recordings

A RedTree capability to store photographs, communications, documents or recordings does not provide legal permission to collect them. Users must comply with applicable recording, privacy, confidentiality, communications and intellectual-property rules.

4. Security testing

Users may not probe, scan, test or circumvent RedTree security without written authorisation, nor attempt to access another user's data or privileges.

5. Protective measures

SIMG may reasonably restrict or suspend access when necessary to stop manifestly unlawful or abusive use, address a serious security risk or comply with law. Suspension does not transfer ownership of user content to SIMG.

6. Contact

contact@thesimg.com | +33 (0)1 59 58 01 53