

Information Security Policy

Public
Version 2.2

For more information please contact:
Information Security

Printed documents or local copies will be classified as uncontrolled documents

Believing in accessibility for all

Document Control

Legal Disclaimer

This document and all the information contained in it is proprietary and confidential to Recite Me. Recite Me reserves all intellectual property rights in relation to the material included in this document. Accordingly, it must not be disclosed or otherwise revealed to outside parties without the prior written consent of Recite Me.

Document Information	
Title	Information Security Policy
Document Reference	ISP-01
Version No	2.2
Classification	Public
Review Period	12 Months
Status	Published
Last updated	19 May 2026
Last reviewed	19 May 2026
Document Owner	
Name | Title	Simon Backwell, Information Security and Data Protection Officer
Updated / Reviewed by	
Name | Title	John Abbott, Head of Product
Recipients	
Name | Title	Recite Me

See end of document for Change History

Contents

1 Purpose 4
2 Scope 4
3 Objectives 4
4 Governance and Certification 5
5 Policy Statement 5
- 5.1 Risk Management 5
- 5.2 Business Continuity 5
- 5.3 Training and Awareness 5
- 5.4 Physical Assets 5
- 5.5 Cloud Services and associated assets 5
- 5.6 Security (Physical and Technical) 6
- 5.7 Security Breach and Incident reporting 6
- 5.8 Systems Development 6
- 5.9 Responsibilities and Sanctions 6
- 5.10 Continuous Improvement 6
- 5.11 Compliance 6

1 Purpose

The purpose of this document is to define and establish the foundations of the Information Security Policy for all Recite Me IT systems, network, equipment, and the data contained in those systems.

The policy and security documentation have been developed in line with the following:

- HMG Security Policy Framework (SPF)
- ISO 27001:2022, “Information security, cybersecurity and privacy protection — Information security management systems - Requirements”
- ISO 27002:2022 “Information security, cybersecurity and privacy protection - Information security controls”
- ISO 27017 “Code of practice for information security controls for cloud services”
- ISO 27018 “Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”.

The establishment and adherence to an Information Security Policy is essential to Recite Me, so that our customers understand our commitment to managing the security of the information Recite Me processes. This policy acts as the top-level document required under clause 5.2 of ISO 27001:2022, mandating all other policies and procedures that Recite Me maintains as part of its Information Security Management System (ISMS).

The term “Information System” is used throughout this policy and is defined as the IT hardware, system and application software, communication components, documentation, physical environment, and the information assets that together form a business domain.

2 Scope

The ISMS applies to all aspects of the work conducted by Recite Me Limited, Recite Me Inc and Recite Me Australia Pty Ltd, who are an Accessibility platform service provider. We provide an Assistive Toolbar, an Accessibility Checker, PDF Accessibility Remediation and Accessibility Auditing. Our offices are located at Baltimore House, Baltic Business Quarter, Gateshead, Tyne and Wear, NE8 3DF (United Kingdom) and 12110 Sunset Hills Road #600, Reston, VA 20190 (United States of America).

This policy applies to all IT resources and equipment managed, supported, owned, or leased by Recite Me. The policy will therefore apply to all employees and anyone else with authorised access to Recite Me IT resources and network services. For all ISMS documents, Recite Me Limited, Recite Me Inc and Recite Me Australia Pty Ltd will be referred to as “Recite Me”.

3 Objectives

Recite Me’s main mission is to provide “accessibility for all.” Doing so via our products and services requires us to ensure we have the appropriate technical and operational measures in place to protect our and our customers’ data. Our security objectives reflect and support that mission.

The Recite Me Senior Management team is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout the company to maintain its competitive edge and to meet its business objectives. To achieve our business objectives, Information Security will set information security objectives which align with and support those business objectives, are consistent with this policy and agreed with the Recite Me Senior Management team. These objectives are reviewed and agreed annually, documented and tracked.

Preserving - All Recite Me employees will be made aware of their responsibilities to information security, to report security breaches and to act in accordance with the requirements of the ISMS.

Confidentiality – The Information we process is only accessible to those with authorised access. By securing the information on a need-to-know basis we prevent unauthorised access, deliberate or accidental changes to the information held.

Integrity - Safeguard the accuracy and completeness of information and processing methods and prevent deliberate or accidental, partial, or complete destruction, or unauthorised modification, of either physical assets or electronic data. Recite Me must comply with all relevant data-related legislation in the jurisdictions in which it operates and processes data.

Availability – Information and associated assets should be accessible to authorised users when required but remain physically secure. The Information System must be resilient and Recite Me must be able to detect and respond rapidly to incidents that may threaten the continued availability of assets, systems, and information.

4 Governance and Certification

The Recite Me Senior Management team govern and are accountable for information security, business continuity and data protection. The Head of Product provides strategic leadership for the ISMS, ensuring that security objectives remain aligned with business goals. Governance is exercised through regular reviews between the Head of Product and the Information Security and Data Protection Officer, with broader departmental leadership convened as necessary to address matters such as document reviews, specific risks or policy requirements. In the Head of Product's absence or at their discretion, the Information Security and Data Protection Officer shall liaise with Senior Management with the necessary delegated authority.

As noted in section 3, Recite Me's mission is to provide "accessibility for all." We are committed to maintaining robust technical and organisational measures to support that mission. To ensure this, Recite Me is aligned to and working towards ISO 27001 certification. Furthermore, Recite Me is certified to Cyber Essentials and Cyber Essentials Plus, both National Cyber Security Centre (NCSC) schemes in partnership with the IASME consortium. These are recertified on an annual basis and can be verified via the IASME Certificate Search.

5 Policy Statement

"Recite Me Information Systems will be available when needed, will be accessed only by legitimate users and will contain complete and accurate information. The Information Systems will also be able to withstand, or recover from, threats to their confidentiality, integrity and availability."

To satisfy this overall policy statement, Recite Me will implement security measures, commensurate with the value of its assets, to protect its Information Systems, with priority given to those systems that are considered critical to the business and its customers. The following statements represent the minimum information security processes and controls applicable to all Recite Me information systems.

5.1 Risk Management

The Recite Me risk management framework provides the context for identifying, assessing, and controlling information-related risks across our internal infrastructure and cloud services. Through the maintenance of our ISMS and BCMS, we utilise the Statement of Applicability (SoA) and risk treatment plans as our primary control mechanisms. These are supported by specialised assessments, such as Business Impact Analysis (BIA), Data Protection Impact Assessments (DPIAs) or Legitimate Interest Assessments (LIAs), which are conducted only where applicable based on the specific nature of the data processing or business activity. This ensures our technical and organisational measures remain proportionate to the identified risks.

5.2 Business Continuity

Recite Me has established a Business Continuity Management System in line with ISO 22301 that is designed to respond to incidents of a minor, moderate, and severe nature lasting for short, medium and long durations of time. Failover of our hosting services will take place at least annually, with other areas being tested at different frequencies (for example, office fire alarm tests). The business continuity policy, testing programme and associated continuity and disaster recovery plans will be reviewed on an annual basis or when significant changes to the infrastructure occur.

5.3 Training and Awareness

All Recite Me employees and third-party suppliers dealing with Recite Me and customer data are expected to comply with the Recite Me security policy and with the ISMS that implements this policy. All employees will receive appropriate training on a range of topics, including, but not limited to, physical and data security, business continuity, social engineering, Artificial Intelligence (AI) and data protection. Third parties will be required to confirm compliance to Recite Me security requirements, whether that is through maintaining their own ISMS and certification, having a security posture that meets our requirements or contractual obligation to maintain a minimum set of standards relating to security, continuity and data protection.

5.4 Physical Assets

All Recite Me employee technology assets will be uniquely identified and recorded within the IT systems. Where Recite Me owns IT assets or applications required for customer use, the Technology team will classify these assets according to the protection levels required to secure them properly.

5.5 Cloud Services and associated assets

Where cloud service providers are utilised for both Recite Me and their customers; the appropriate ISO 27017 and 27018 controls have been documented in the Recite Me Statement of Applicability and will be used to enforce and secure both

business and customer information across the Recite Me IT infrastructure and external resources. In choosing the appropriate cloud services, Recite Me will take the appropriate security due diligence to ensure that services used meet applicable legislation and regulations.

5.6 Security (Physical and Technical)

Physical - assets, such as computer hardware, must be located with due consideration given to their value in security terms and following an assessment of the relevant risks.

Technical - There must be measures in place to protect Recite Me information systems from viruses, other malicious software, and data loss prevention (DLP). User access will be monitored and reported accordingly using appropriate threat analytics tools and all information systems will be monitored for potential security incidents and / or breaches.

5.7 Security Breach and Incident reporting

All actual, attempted, or suspected security incidents or breaches must be reported to Information Security. Similarly, any malfunctions, threats and weaknesses that could compromise the security of Recite Me information systems must also be reported to Information Security. The reporting and management of such security issues will be in accordance with the laid down procedures and in accordance with applicable legislative and regulatory requirements.

5.8 Systems Development

All business cases or feasibility studies for new projects are to include estimated costs for Information System security. The nominated Project Owner, alongside the Information Security and Data Protection Officer, will be responsible for producing and implementing effective security countermeasures and producing all relevant security and data protection documentation, security operating procedures and contingency plans as part of each project.

5.9 Responsibilities and Sanctions

The Recite Me Senior Management team has ultimate responsibility for the security of Recite Me Information Systems and information assets. That responsibility is delegated to the appropriate managers for the day-to-day security requirements. Reporting to the Head of Product, who sits on the Recite Me Senior Management team, the Information Security and Data Protection Officer is responsible for the operational maintenance and daily requirements related to security, continuity and data protection.

All Recite Me employees have a requirement to understand Recite Me security requirements and the Recite Me Information Security Management System. Recite Me employees are informed that irresponsible or improper actions that breach the security policies, procedures and work instructions will result in disciplinary action. Where a member of staff is found to have broken the law, the matter will be dealt with by the appropriate authority and may lead to a criminal prosecution.

5.10 Continuous Improvement

Recite Me will ensure that policies, procedures and controls are regularly reviewed and enhanced. Recite Me will continue to review customer, legislative and regulatory requirements, new certifications, and best practice and guidance updates, to ensure continuous improvement of our security posture against new risks or threats.

5.11 Compliance

Recite Me will comply with all contractual requirements, laws, statutory requirements and legislation that are relevant to its Information Systems, including both UK and EU General Data Protection Regulation (GDPR). Further details are available within the security manual, SoA and procedures.

Whilst Recite Me does not meet the criteria under Article 37 of GDPR to require a Data Protection Officer (DPO), the Information Security and Data Protection Officer holds that position. The Information Security and Data Protection Officer acts in accordance with Article 38 of GDPR.

Simon Backwell, Information Security and Data Protection Officer | John Abbott, Head of Product

Date: 19th May 2026





Change History

Version No.	Date	Updated / Reviewed by	Page(s)	Section(s)	Description of update
2.0	11 Aug 2023	Nathan Smith	All	All	Rewrite of policy, first issue
2.0	28 Aug 2024	Nathan Smith	All	All	Policy review, no change
2.1	26 Mar 2025	Nathan Smith	All	All	Minor wording update
2.2	29 Apr 2026	Simon Backwell	All	All	Full rebrand and rewrite for internal and external audiences, amended document reference in keeping with new reference scheme.
2.2	19 May 2026	John Abbott	All	All	Updated policy reviewed and signed off