

# Information Security Policy

## About this policy

### Purpose

RNIB is committed to delivering effective information security such that the confidentiality, integrity, and availability of information is maintained throughout the organisation. This policy sets out how we do so, and how we will comply with regulatory, legal, and contractual obligations.

### Benefits of having a policy in place

This policy seeks to provide the following benefits:

* Protect RNIB from liabilities or damages by informing the organisation of its statutory and contractual obligations relating to information security.
* Ensures that RNIB users are aware of their information security and information risk management responsibilities
* This policy and its subsidiary policy set, standards and procedures are developed to follow security best practices reflective of a secure working environment and representative of a security aware culture
* Enable RNIB to respond to changes in the context of the charity as appropriate, initiating cycles of continuous improvement
* Demonstrate the structured approach RNIB takes towards delivering and maintaining security solutions across technology, people, and processes
* Help to establish security minded working groups to identify issues and risks, enabling proportionate remediations to be agreed and implemented

### Embedding this policy

This policy is a mandatory training article within the Information Security Management System (ISMS) and RNIB’s organisational policy review set. This policy must be read and understood by all RNIB staff, contractor/temp workers, and volunteers within 4 weeks of joining RNIB, and annually thereafter. The latest approved version of this policy is available in the Policies SharePoint library [here](https://rnib.sharepoint.com/sites/DocumentControl/Shared%20Documents/Forms/AllItems.aspx).

Completion rates are monitored by the Information Security Team, Organisational Development (OD) and RNIB’s Leadership Group.

On a monthly and quarterly cycle, the Information Security Team, led by the Head of Information Security provide information security performance and assurance reports to the Chief Financial Officer (CFO), Director of Technology and Technology Management Team.

Information security risks and associated assurances are reviewed at least quarterly to ensure they remain relevant and that treatment plans are progressing. Additionally, findings from internal and external audits are tracked monthly by the Compliance, Risk and Assurance Team and reported through to the Audit, Risk and Assurance Committee (ARAC).

### Risks and Implications

Failure to comply with this policy could compromise the confidentiality, integrity and/or availability of RNIB information including data held on IT systems or paper-based articles. This includes information about colleagues, customers and third parties. In the worst-case scenario, permanent loss of data and/or services is a potential consequence of non-conformity.

Failure could also expose the charity to; reputational damage, contractual breaches, regulatory and/or statutory investigation and significant fines, the inability to accept payment card information, and monetary losses such as donations and incident recovery costs.

### Scope

#### Who does this policy apply to?

This policy applies to all employees, volunteers, contractors, consultants, temporary and other workers at RNIB and its subsidiary companies and charities (as listed in Appendix 1).

This policy also applies to all third parties who have authorised access to RNIB-owned IT systems and are exposed to RNIB confidential, sensitive, or restricted information to deliver a service.

In alignment with the ISMS, third party suppliers processing information on behalf of RNIB must read and understand the Third-Party Information Security Policy. This is to ensure as a service provider, they understand and comply with RNIB’s minimum information security standards.

#### What does this policy apply to?

This policy applies to everything we do with information and the information assets used to interact with data, including but not limited to; paper articles, networks, and IT systems (i.e., servers, workstations, applications, and documents), cloud platforms, mobile devices, USB sticks etc. This includes assets owned by RNIB or leased from an approved third-party vendor.

### Exceptions to this policy

Any exception to this policy must be agreed by the relevant Data Owner (this is likely to be the Information Asset Owner if known) and the Head of Information Security. In case of disagreement, this must be escalated to the Senior Information Risk Owner.

### Roles and responsibilities

All employees, volunteers, contractors, consultants, and other parties working for or on behalf of RNIB have an individual responsibility for ensuring information security.

Key roles and responsibilities are set out in Appendix 2. For more detailed information and a view of the complete list, please request to see the ISMS-SPE-DOC-1-3 ISMS Roles and Responsibilities Matrix.

### Definitions

Availability – in the context of this policy means the ability for authorised users to access resources and data whenever required for their role or in pursuit of using RNIB services.

Critical information - any information or data considered confidential, sensitive, or restricted. This also includes information supporting the successful operation of critical RNIB services.

Data – often used interchangeably with “information” is information that has been translated into a form that is efficient for storing, moving, or processing by computer systems.

Confidentiality – in the context of this policy refers to ensuring only authorised users are given access or permission to view/modify systems and data.

Information – often used interchangeably with “data” is organised or classified data which has some meaningful value to those using it. When information is entered into and stored in a computer, it is generally referred to as data. After processing, such as formatting and printing, output data can again be perceived as information.

Information Security Management System (ISMS) - is a set of policies and procedures for systematically managing the information RNIB collects, produces, and processes. The ISMS is aligned to the ISO/IECS27001: 2013 international standard and the goal of the ISMS is to minimise risk and ensure business continuity by pro-actively preventing and limiting the impact of security breaches.

Integrity – in the context of this policy refers to maintaining the trustworthiness of data by having it in the correct state and immune to any improper modifications.

PCI-DSS - Payment Card Industry Data Security Standard

Personal data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing - any operation or set of operations which is performed on information, data or on sets of data, whether by automated means or not, such as collection, viewing, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Security incident - is an event that may indicate that the confidentiality, integrity and/or availability of systems or data have been compromised or that measures put in place to protect them have failed.

Vital assets – IT devices which are key to the successful operation of critical RNIB services, including core infrastructure systems and devices used to store/process critical information.

## Statements of the Policy

### RNIB is a responsible organisation who recognises the importance of information security

RNIB is a charity with focus on driving societal change and providing support services for blind and partially sighted people. The storage and processing of confidential customer information is part of our core obligation. It is therefore RNIB’s duty to protect this data and other RNIB information, which is considered confidential, sensitive, or restricted.

Senior management including Trustees, members of the Audit, Risk and Assurance Committee (ARAC) and the Executive Leadership Team (ELT) have a common goal and commitment to delivering and sponsoring effective information security throughout RNIB.

As such, RNIB has chosen the established and industry-recognised ISO 27001 standard as the preferred framework to align its Information Security Management System (ISMS) to.

### Individuals must take responsibility for keeping information assets secure from unauthorised access, damage, loss and theft

Employees are given individual RNIB accounts and equipment for completing work and/or representing RNIB. Employees must not share user account passwords or their RNIB devices with anybody else, including family members or work colleagues.

Devices must be secured when not in use and procedures followed to securely dispose of equipment and data that is no longer required, broken or unusable. Devices require ongoing maintenance to ensure they operate optimally and securely. Asset holders/owners must co-operate with the Technology Team regularly to patch and reboot systems and applications.

RNIB information must not be created or stored locally on personally owned electronic devices unless it is classified as public or being used within an RNIB approved application which are made available for staff to use in scenarios where personal devices are necessary to carry out work duties (i.e., volunteering).

### Current and emerging information risks must be managed effectively

Processes and tools are in place to allow for the timely identification of vulnerabilities and risks. If a risk or security issue is newly identified, it must be logged, assessed, and remediated according to agreed risk appetite levels.

The Head of Information Security will provide resource to support information security risk assessments at the request of colleagues. Lead times vary from a few days to a few weeks during busy periods. The Compliance, Risk & Assurance Team is responsible for monitoring risk management practices and demonstrating information security assurances to key senior stakeholders.

Third parties are key to the delivery of many services at RNIB. Procedures must be followed to manage the information risks posed by third party suppliers and their solutions.

### Access to information must be appropriate and proportionate to the role being carried out

Authentication technology is used to validate the identity of users accessing RNIB resources and information.

Dedicated identity verification procedures must be adopted to validate the identity of individuals before confidential information is shared. This is particularly important in instances where technology is unable to authenticate and validate the identity of individuals. For example, this may apply where a customer calls to discuss their account with RNIB.

Access to systems and information must be centrally controlled by Technology where possible and role-based access controls implemented. Access requests to resources outside of standard role-based access controls must be approved by respective Data Owners as a minimum before access is granted. Periodic access reviews must be carried out by Line Managers, system and/or Data Owners otherwise known as Information Asset Owners (IAOs).

### Security controls adopted must be proportionate to the services and information being protected and will not unnecessarily impact the user experience

Physical, procedural, and technical controls implemented must balance user experience and security requirements. Where conflicts arise that cannot be resolved, an escalation should be made to the Senior Information Risk Owner (SIRO) to support decision making.

### IT infrastructure, systems and solutions must be selected, designed and built with operational resilience and security in mind

Development and test environments must be segregated from production environments, and live data containing personal customer or employee information must be made anonymous before being used for testing.

Adequate physical and environmental technologies must be implemented and maintained to ensure that vital assets are protected from environmental hazards and physical security breaches.

Only approved technologies or technology changes shall be implemented in the RNIB environment. The Business Design Authority (BDA), the Technical Design Authority (TDA), the Project Management Office (PMO) and Technology’s Change Advisory Board (CAB) are key groups that should be engaged to review and approve new solutions or technology changes (dependent on scope, context and impact of proposal).

All third-party suppliers processing RNIB critical information must abide by the RNIB Third Party Information Security Policy and be able to demonstrate the existence of security controls providing equivalent or higher levels of assurance.

In case of a critical/major incident, disaster recovery and business continuity plans must be in place and maintained by the business. These plans should be tested periodically to ensure effective operational resilience.

### Effective security monitoring must be implemented and security incidents effecting information assets reported, managed, and resolved without undue delay

All RNIB IT systems are subject to logging and monitoring to enable suspicious activity to be identified, responded to and incidents prevented. Where possible, non-intrusive methods must be used and access to log data restricted.

Colleagues are reminded that devices are issued for work purposes and are not setup to facilitate personal activities. If colleagues use their device for personal reasons that are considered reasonable (e.g., paying a utility bill, checking your bank account), they do so at their own risk. For more information, please refer to the RNIB Acceptable Use Policy.

All suspected or confirmed security incidents must be reported immediately to the Information Security Team via the IT Helpdesk by calling 01733 375 375. All incidents must be handled in line with defined incident management procedures. In cases where discretion is needed, please contact the Head of Information Security directly or a member of the Senior Leadership Team (SLT).

Incident information is considered sensitive in nature and must not be shared with unauthorised individuals or members of the public. Where an incident requires further communication with customers, regulators, police, or other authorities, it must be managed and communicated in accordance with protocols defined by Internal Communications, Information Governance and Legal.

### A responsible, information security aware culture must be maintained across the organisation

All employees must complete the mandatory training assignments delegated in MetaCompliance (internally known as MOLLIE) within 4 weeks of starting and annually thereafter. This includes but is not limited to the following:

* Privacy and Security Basics training
* Cyber Security training
* Information Security Policy review
* Data Protection Policy review

Ad-hoc training will be delivered to colleagues in response to breaches, incidents and phishing simulation campaigns.

Whilst using RNIB information assets, colleagues must not behave in a way that could suggest that they’re trying to develop a personal relationship with a child or vulnerable adult. Individuals must not post any content that could be deemed defamatory, obscene, or libellous. Additionally, individuals must not post comments or send messages that exhibit or appear to endorse grossly irresponsible behaviour or law breaking of any kind. Please see Appendix 3 for further guidance on appropriate and inappropriate behaviour.

### Information must be collected and processed for legitimate business purposes only

Information shall only be retained for as long as it is needed; for legitimate business purposes; and in accordance with any contractual, statutory retention period or legal requirement.

### Applicable UK laws and regulations must be complied with at all times

Gateshead delivers a critical function to the blind and partially sighted community and within its suit of services, holds a Customer Data Environment (CDE) which is segregated and considered a high security zone. Due to the sensitive nature of information processed within this environment, the Gateshead CDE is PCI-DSS Level 1 certified. Any individual working in this environment must understand the conditions and requirements of this standard through completing dedicated training courses.

RNIB holds and processes the personal data of customers, staff, third-party suppliers, donors, and volunteers where it is lawful to do so, in line with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. RNIB’s governance arrangements, roles and responsibilities, and practices for the handling of personal data are set out in the IS-02.00 Data Protection Policy.

Colleagues must recognise the implications of behaving unlawfully when using RNIB systems and information. The Computer Misuse Act 1990 criminalises several acts, including accessing data without authorisation (i.e., hacking) and installing malware (e.g., computer viruses, spyware, or ransomware) on a person's computer. In cases where this law is found to be breached, the Head of Information Security must report the crime to the police and support investigative efforts.

### The workforce is committed to delivering on information security commitments contractually agreed with customers and third parties

Information security controls must be in place, reflecting the requirements set out in customer and third-party contracts. A representative from the Information Security team must review and approve the information security-related terms and conditions set out in contracts and agreements before such documents are agreed and services provisioned. This is to ensure that RNIB is able to meet expectations and any issues identified are addressed pro-actively.

The Commercial Team is responsible for referring for triage customer security requirements to the Technology Team as they become known.

## Compliance

Any violation of this policy will be investigated and if the cause is attributed to wilful disregard or negligence, it may be treated as a disciplinary offence. All disciplinary proceedings will be coordinated through HR. In serious cases this may lead to dismissal for gross misconduct for employees, or termination of contract for contractors and agents, or termination of volunteer status for volunteers. Any breach of law may also result in criminal prosecution or civil action.

## Review

This policy is due for review every year or following any relevant and significant organisational or legislative change if earlier.

Next review date: 24/08/2023

## Document Owner and Approval

Document owner: Iayesha Reid – Head of Information Security

Final policy sign off by: Board of Trustees

## Associated Policies, Procedures, Standards and Guidelines

This policy is associated with the following RNIB policy documents of the ISMS:

* IS-00.01 Information Security Risk Management Policy
* IS-01.01 Asset Management Policy
* IS-02.00 Data Protection Policy
* IS-03.01 Access Control Policy
* IS-04.01 User Lifecycle Policy
* IS-04.02 Acceptable Use Policy
* IS-04.08 Acceptable Use Policy for Stand-Alone Development and Testing Machines
* IS-05.01 Information Security Operations Policy
* IS-05.12 Mobile Device Management Policy
* IS-05.13 Bring your own device (BYOD) Policy
* IS-06.01 Cryptography Policy
* IS-7.01 System Acquisition, Development and Maintenance Security Policy
* IS-08.02 Third Party Access Policy
* IS-11.01 Information Security Incident Management Policy

This policy addresses the controls outlined in Annex A.5 of ISO27001:2013.

## Appendices

### Appendix 1 – RNIB Subsidiaries

RNIB currently has nine subsidiary charities and companies (of which RNIB is the sole shareholder/member and are therefore wholly owned by RNIB). These are:

* RNIB Charity
* RNIB Enterprises
* RNIB Services Limited
* RNIB Direct Services Lottery Limited
* RNIB Feel Good Friday Lottery Limited
* Action for Blind People
* Blind Centre for Northern Ireland
* Talking Newspaper Association of the United Kingdom
* National Library for the Blind

### Appendix 2 – Information Security Roles and Responsibilities

**Information Security Team**

* Maintain oversight and ownership of the suite of documents making up RNIB’s ISMS.
* Monitor and provide assurances to key stakeholders that policy requirements are upheld and adopted.
* Manage and triage risks and remediation activities reported internally or via audits and assessments.
* Guide and support the organisation to protect information, upskill the workforce and effectively respond to incidents.
* Implement technological and/or procedural controls to protect information on balance with risk exposure and appetite levels.
* Monitor, review and adjust the ISMS and controls in place through the principle of continuous improvement.

**Line Managers**

* Ensure staff have appropriate, role-based access to RNIB resources.
* Ensure leavers and movers are processed accordingly to avoid unauthorised or excessive access to systems and data.
* Ensure that staff, volunteers and temporary workers receive adequate training and guidance on this policy, as well as others within the ISMS policy set.
* Support staff to complete education and awareness courses issued by Organisation Development and Information Security.

**Senior Leadership Team**

* Support and uphold this policy and act as a point of escalation for major or sustained breaches in policy.
* Monitor and resource the necessary activities, in keeping with other business priorities.
* Ensure that feedback is provided to the Document Owner if necessary and support the Document Owner in regular reviews.

**Senior Information Risk Owner**

The Senior Information Risk Owner (SIRO) is the executive sponsor for privacy and security at RNIB and is the Chair of the Information Governance Group (IGG). The Chief Financial Officer (CFO) acts in this role. In this role, they:

* Provide strategic guidance and input to Management and Executive Leadership Team discussions.
* Take ownership and ensure the implementation of RNIB’s information risk approach, related policies and risk assessment processes.
* Act as an advocate of information risk, governance and security.
* Advise the Chief Executive and Board of Trustees on any public information risk statements or reports they issue.
* Provide executive ownership of RNIB’s information incident management framework.
* Act as final arbiter / decision maker for any information security issues that cannot be resolved by the Information Security Review Group (ISRG).

### Appendix 3 – Appropriate and Inappropriate Behaviours

Content in the following table provides guidance about activities that are deemed appropriate and inappropriate.

(Table; two columns, one row)

Table 1 - Appropriate versus inappropriate behaviour

|  |  |
| --- | --- |
| **Appropriate**1. Setting up privacy and multifactor authentication settings for any social networking site used for RNIB activity.2. Using dedicated, professional, and individual accounts for conducting RNIB activities (i.e., when making contact with service users, their families and other professionals).3. Making sure that all information about you is accurate and appropriate.4. Remaining professional through all forms of communication. Online conversations such as “chat” or “instant messaging” are considered written documents that will be stored (subject to retention periods) and should always be treated as such.5. If you are unsure who can access information you plan to upload to an online platform, assume it is public until it is known. 6. Use your mobile device or camera to record work purpose images where it is not possible to identify any customers or staff members. If people are identifiable in an image, then the image must not be stored or utilised without written consent of the individual or appropriate responsible adult. | **Inappropriate**1. Giving your personal information to service users - children/young people, their parents/carers. This includes mobile phone numbers, social networking accounts, personal website/blog URLs, online image storage sites, passwords, etc. Your assigned RNIB landline DDI number will work on your mobile device through the Horizon App.2. Using any form of communication to send personal messages to vulnerable adults or children/young people.3. Sharing your personal details with service users on a social network site.4. Adding/allowing a service user to join your contacts/friends list on personal social networking profiles.5. Using your own digital camera/video for work. This includes integral cameras on mobile phones.6. Playing online games with service users.7. Discussing sensitive or personal content in a public place where you might be overheard.8. Sharing assigned logon credentials (username and password) with peers to cover annual leave. |

## Version control

The table below shows the history of the document and the changes that were made at each version:

The table has five columns and fourteen rows, first row headings.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author & Job Title | Changes | Status & Level of Approval |
| 0.1 | 26-02-20 | Ben Wilkinson | Authoring |  |
| 0.2 | 28-02-20 | Patrick McCarty | Minor changes |  |
| 0.3 | 10-03-20 | Ben Wilkinson | Minor amendments to policy statements. Update of Document control to RNIB standard. |  |
| 0.4 | 03-04-20 | Neil Beckingham | Minor amendments to policy statements 2.10 |  |
| 1.0 | 03-04-20 | Neil Beckingham | Approval |  |
| 1.1 | 15-04-20 | Ben Wilkinson | Additions to Section 6 Associated Policies.  |  |
| 2.0 | 21-05-20 | Board of Trustees | Approved |  |
| 2.1 | 14-08-20 | Approved by Director of Digital Transformation | Additional content added into section 2.4 Safeguarding and Information Security re Information Creation on Devices |  |
| 2.2 | 29-03-21 | David Mann | Document review cycle, updated with minor amendments |  |
| 2.3 | 30-09-21 (Approved 13-10-21) | Iayesha Reid | Document updated to include high-level objectives and removal of lower-level operational content found to be inappropriate due to duplication in other subsidiary policies |  |
| 2.4 | 06/01/22 | Iayesha Reid (Bruce Dickinson) | Amended incorrect text and typo in para 2.2. |  |
| 2.5 | 27/05/22 | Iayesha Reid & Dan Jackson | Annual review and refresh of content throughout |  |
| 3.0 | 24/08/22 | Iayesha Reid (Head of Information Security) | Reformatted and updated throughout post ARAC review | Approved by Board of Trustees 22 September 2022 |
| 3.1 | 10/10/22 | Iayesha Reid (Head of Information Security) | Text reformatted to left-alignment |  |

## Document control

The table has two columns and nine rows.

|  |  |
| --- | --- |
| **Document title** | IS-00.00 Information Security Policy |
| **Document owner** | Head of Information Security, Information Security - Technology |
| **Originally approved by** | Board of Trustees |
| **Originally approved on** | 21 May 2020 |
| **Approved by** | Board of Trustees |
| **Approved on** | 22 September 2022 |
| **Planned review date** | August 2023 |
| **Is document published internally or on RNIB public-facing website?** | Internal |
| **Version no.** | 3.1 |

End of document