cookRNIB See differently Logo

# Data Protection Policy

## About this policy

### Purpose

RNIB is committed to respecting the privacy and confidentiality of all customers, staff and volunteers.  This policy sets out how we do so, and how we will comply with Data Protection legislation.

### Benefits of policy being in place

This policy sets out RNIB’s statutory responsibilities under data protection legislation.

### Embedding this policy

The policy is supported by existing processes and training. It is overseen by the Information Governance Group, and assurance reporting is brought to this group monthly.

### Risks and Implications

Failing to adhere to data protection legislation and good practice could put RNIB’s customers at risk. A breach of data protection, or failure to demonstrate good practice could put RNIB at risk of significant financial penalties as well as reputational damage.

### Scope

#### Who does this policy apply to?

This policy applies to anyone who accesses or uses RNIB data about customers, staff or volunteers.

It also applies to all of RNIB’s subsidiary companies and charities that process personal data (as listed in Appendix 3 of this policy).

#### What does this policy apply to?

This policy applies to everything we do with information that identifies any living person. This includes how we collect, store, share, use and destroy such data.

### Exceptions to this policy

Any exception to this policy must be agreed by the relevant Information Asset Owner (See Appendix 1) and the Data Protection Officer. In case of dispute, this must be escalated to the Senior Information Risk Owner.

### Roles and responsibilities

Roles and responsibilities are set out in full in Appendix 1.

### Definitions

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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, 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.

Data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

## Statements of the Policy

### RNIB and subsidiaries are registered data controllers

RNIB makes decisions about how personal data is processed, and has agreements in place with its subsidiaries about how their data is processed and shared.   The ICO registration details of RNIB and each subsidiary are set out in Appendix 3.

### RNIB has clear roles and responsibilities to manage data

RNIB has a governance structure and written roles and responsibilities for the management of personal data. These are set out in Appendix 1.

### RNIB will be transparent about our reasons for processing people’s data

We hold records of the reasons for which we hold and use personal data through our Records of Personal Data Processing Activities (ROPA). The ROPA is owned and maintained by each Information Asset Owner and overseen by the Information Governance Team. The ROPA holds a full account of where data is held, as well as RNIB’s legal basis for processing data as part of each business activity.

We will provide clear information to customers and staff about what we do with the data we hold about them through our Privacy Notice, which is published online.

### RNIB will respond to all queries about Data Subjects Rights

All individuals have legal rights relating to the information that we hold about them. These are set out in law, and can be found in Appendix 2. The Information Governance Team is responsible for the group-wide processes to deliver data subjects’ rights.

Requests for copies of personal data, or complaints about the way that RNIB has processed people’s personal data, must be forwarded to the Information Governance Team by emailing: dataprotectionofficer@rnib.org.uk

### RNIB will manage people’s data securely

We will take appropriate measures to prevent unauthorised processing of personal data, accidental loss or destruction of, or damage to, people’s personal data. Information relating to our customers, staff and volunteers is stored securely and only made accessible to authorised and trained staff and volunteers.

RNIB has a set of Information Security policies as well as a Physical Security Policy which can be found in [RNIB’s policy site](https://rnib.sharepoint.com/sites/DocumentControl/Shared%20Documents/Forms/AllItems.aspx). These set out the standards we apply to how data is stored and accessed, along with our security standards, including the use of passwords and encryption.

RNIB will conduct a [Privacy Risk Assessment](https://rnib.sharepoint.com/sites/InformationGovernance/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FInformationGovernance%2FShared%20Documents%2FGeneral%2FPrivacy%20Risk%20Assessments&viewid=6166af73%2Da0ce%2D4d38%2D9548%2Db45d11ad4dce) when changing the way personal data is collected, stored or used.

RNIB will ensure that business continuity measures are in place for our information assets. Business continuity measures will be agreed on a risk basis, and are owned by RNIB’s Major Incident Response Team (MIRT).

### Management of breaches, incidents and near misses

#### 2.6.1 Any suspected incident or breach must be reported

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of our information, in any format, or IT systems in which this information is held. Any suspected breach or incident must be reported immediately by emailing the data protection mailbox: dataprotectionofficer@rnib.org.uk

If the incident clearly relates to the functioning of an IT system, or an IT failure or concern, you must contact the IT helpdesk directly by phoning: 01733 375375

#### 2.6.2 The Information Security Manager

The Information Security Manager is responsible for leading the investigation and resolution of incidents that relate to IT systems and network security incidents and suspected breaches of RNIB’s Acceptable Use Policy.

These will be managed in line with the Information Security Incident Policy.

In all cases where a suspected incident involves personal data, they or their nominee will inform the Information Governance Manager immediately to investigate and resolve the issue.

#### 2.6.3 The Information Governance Manager

The Information Governance Manager, who is also the Data Protection Officer, is responsible for investigating and recommending appropriate action in response to any suspected breaches of personal data security and will have oversight of action to be taken in response to loss or compromise of personal data, or systems and devices containing such information.

* In the case of any incident that involves personal data, the Information Governance Manager will request that an Incident Form is completed.
* The Information Governance Manager is responsible for liaising with the Information Commissioner’s Office and reporting breaches in line with regulatory requirements to report any data breach that is likely to result in a risk to the rights and freedoms of data subjects within 72 hours of discovery.

#### 2.6.4 Defining and reporting a ‘personal data breach’

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service ”.

A personal data breach may mean that someone other than the data controller gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller’s own employee accidentally alters or deletes personal data.

A breach of personal data will be notified to the Information Commissioner’s Office through its online form within 24 hours of discovery.

Other regulators, including the Charity Commissioners, will be notified of data breaches or security incidents as appropriate.

#### 2.6.5 Learning from incidents, breaches and near misses

The Information Security Manager and Information Governance Manager will provide regular reporting to the Information Governance Group and the Executive Leadership Team.

### RNIB will ensure that Direct Marketing is compliant with legislative requirements

All direct marketing must be reviewed and approved by the Direct marketing group. All staff must contact directmarketingreports@rnib.org.uk if planning direct marketing.

### RNIB will ensure all staff understand their responsibilities

The Information Governance Manager will produce and manage a [Training Needs Analysis](https://rnib.sharepoint.com/%3Aw%3A/r/sites/InformationGovernance/_layouts/15/Doc.aspx?sourcedoc=%7B56F7AD9B-068A-4CC8-A645-49675B09505B%7D&file=2021-22%20-%20Training%20Needs%20Analysis%20V3.docx&action=default&mobileredirect=true), which will set out the privacy and security training required by each group of staff in RNIB, and the frequency of such training.

The Information Governance Group will maintain oversight for the delivery of training against the Training Needs Analysis.

Information Asset Owners are responsible for making sure that staff in their areas complete this training, and that staff understand how this applies to their work

RNIB will hold auditable training records for completion of Privacy and Security training. Reporting of training uptake will be provided to the Information Governance Group and the Executive Leadership Team

Formal training will be supplemented with communications campaigns to draw attention to changes or areas of specific risk.

### RNIB will ensure that third parties process personal data in line with a written agreement

In any case where a third party collects, stores or manages personal data on our behalf, RNIB will ensure that there is a written agreement in place with that organisation, which must be reviewed by RNIB’s Legal team.

### Data Protection and Safeguarding

Every member of staff has a role to play in RNIB’s Safeguarding approach. Any member of staff who has a safeguarding concern must record the information or allegation briefly, factually and accurately and then follow RNIB’s Safeguarding Policy

## Review

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

Next review date: 31/5/2023

## Document Owner and Approval

Document owner: Sinead Mulready – Information Governance Manager

Final policy sign off by: Director of Finance

## Associated Policies, Procedures, Standards and Guidelines

A series of supporting procedures, standards and guidance are set out below and can be found through the [following link.](https://rnib.sharepoint.com/sites/DocumentControl/Policy%20Supporting%20Documents/Forms/AllItems.aspx?newTargetListUrl=%2Fsites%2FDocumentControl%2FPolicy%20Supporting%20Documents&viewpath=%2Fsites%2FDocumentControl%2FPolicy%20Supporting%20Documents%2FForms%2FAllItems%2Easpx&id=%2Fsites%2FDocumentControl%2FPolicy%20Supporting%20Documents%2FInformation%20Governance&viewid=a084ebc3%2Dd36a%2D4086%2Da283%2Dfbfb7c987362)

* Reporting a breach or incident form
* Data Subject Rights Guidance
* Data Transport Standard
* Building checks - data security
* Guidance and standards for data sharing
* Redaction standard
* Returned mail standard
* Ad hoc data sharing with regulatory bodies standard
* Lawful bases for processing data
* Privacy Risk assessment template and guidance
* Transferring or closing a service - guidance and checklist

## Appendix 1 Privacy and Security Roles and Responsibilities

### Senior Information Risk Owner

The Senior Information Risk Owner is the executive sponsor for privacy and security at RNIB, and is the chair of the Information Governance Group. The Director of Finance, Performance and Technology 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 and governance
* Advise the Chief Executive or Head 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 governance issues that cannot be resolved by the Information Governance Group.

### Information Asset Owners

Information Asset Owners must be of sufficient seniority to carry out the role. In RNIB, Heads of Service who report directly into a member of the Executive leadership Team are designated as Information Asset Owners (IAOs). If there is a gap in cover for any reason the Director is responsible until another member of staff of sufficient seniority is appointed or identified.

As a Head of Service, Information Asset Owners are accountable for the management of the business processes in their areas, and for oversight of the staff, contractors and volunteers in their areas.

In the role as IAO, they are accountable for the way in which data is used for these business processes, for the way in which staff use personally identifiable information, and for making sure that their business processes are carried out in line with legislative requirements and RNIB policies.

The core responsibilities of the IAO are to:

* Understand what information, and in particular what ‘personal information,’ is necessary to carry out the business processes in their area
* Make sure that the staff, contractors and volunteers in their area complete mandatory training
* Identify additional training that may be needed by the staff in their area
* Engage with the Information Governance Group regularly to share good practice and understand common risks across RNIB
* Make sure that the staff, contractors and volunteers in their area understand how personal information is to be used – and not used – for business purposes
* Make sure that the staff, contractors and volunteers in their area have access to the right information required for their roles, and not to any more information than is necessary
* Make sure that the requirements of RNIB policies are reflected in their business processes
* Make sure that changes to the way personal data is used, stored or processed are risk-assessed, and that risks are reviewed with the Information Governance Team, and approved by the Senior Information Risk Owner where necessary.

IAOs need to be able to answer the following questions:

* Do I understand what information assets I am responsible for (including personal and non-personal data) and has that understanding been properly documented and shared with the SIRO and others that need that information?
* Have I assessed and logged information risks to those assets?
* Do I have a plan for managing risks, and maximising opportunities for using my information assets?
* Do my team(s) and third parties understand their roles and responsibilities in managing those risks and opportunities?

Types of risks that IAOs must address:

* Staff, contractors and outsiders may access them inappropriately, or disclose them to others.
* Inappropriate access to, or disclosure of, confidential information or personal data by staff, contractors and outsiders, whether accidental or deliberate.
* Inappropriate data sharing – too much or irrelevant data is shared internally i.e. a full list with all personal data is provided where only numbers of a specific category have been requested.
* Internal threat – staff acting in error or deliberately, or external parties obtaining information illegally and exposing it or using it to defraud RNIB or our customers.
* Information loss – particularly during transfer or movement of information, or as a result of business change.
* Records management – that information assets are not retained for longer than required (either by law or for business need) as outlined in the corporate retention and disposal schedule.
* Business continuity/disaster recovery – that the relevant personnel are aware of the agreed continuity and recovery for their services.
* Loss of digital continuity – i.e. losing the ability to use our information in the way required, when required. This means that we should be able to find, open, work with, understand and trust the information. The lifecycle of a piece of information – and how long you need to use and keep it – is often different to the lifecycle of the IT system that is in place to access and use the information.
* Poor quality of information and quality assurance, for example, of datasets.
* Poor change management – business needs change, systems change. Information risk management may change and policies and processes must be kept up-to-date accordingly.

### The Information Governance Group

RNIB has an established Information Governance Group (IGG). It is chaired by the SIRO and its membership is Information Asset Owners from across RNIB. It is supported by the Information Governance Team.

**Information Leads**

Information Asset owners should nominate Information Lead(s) to support them with privacy and security compliance in their area.

Information Leads will be expected to:

* Act as departmental leads for RNIB’s compliance with Data Subjects Rights.
* Attend information sharing sessions with the Information Governance Team, IAOs and other Information, and disseminate relevant messages to IAOs.
* Attend training as required.

### Information Security Manager

* Report to Information Governance Group on information security risks or events as relate to information governance or information processing
* Accountable for the creation, maintenance and implementation of information security policies
* Regularly meet and liaise with Information Asset Owners
* Provide risk assessment and technical guidance on information processing activities and proposals
* Responsible for the implementation of information governance related information security requirements and for information security management
* Ensures technical aspects of information processing are compliant with relevant legislation and regulations.

### Head of Technology

* Ensures information governance policies and procedures are embedded in IT service delivery
* Responsible for the effective management and security of IT resources
* Developing and implementing an IT Disaster Recovery Plan in line with business requirements
* Act as information asset owner for IT infrastructure used in the provision of services and the processing of personal information.

### Data Protection Officer

* Report to Information Governance Group on Data Protection compliance status and major activities
* Liaise on behalf of RNIB with external regulators or other external bodies with regard to privacy issues
* Accountable for the creation and maintenance data protection policies and standards
* Review and quality assure Privacy Risk Assessments for significant personal data processing
* Carry out audits on personal data processing
* Regularly meet and liaise with Information Asset Owners
* Manage responses to Data Subject Access Requests
* Maintain Data Protection risk register

### Head of Legal

* Provide legal analysis of information processing activities and developments
* Provide review services for new information processing activities
* Ensures information processing is compliant with relevant legislation and regulations

### Caldicott Guardian

* Ensure RNIB meets practical, consistent standards for handling patient identifiable information
* Facilitate and enable appropriate information sharing in relation to patient identifiable information in order to benefit or improve service delivery; make decisions thereof
* Champion information governance requirements to ELT when related to patient identifiable information
* Ensure patient confidentiality issues are appropriately reflected in organisational strategies, policies and procedures
* Provide executive oversight over all arrangements where confidential patient information may be shared with external entities.

##  Appendix 2: The Rights of Data Subjects

* To make subject access requests regarding the nature of information held and to whom it has been disclosed.
* To prevent processing likely to cause damage or distress.
* To prevent processing for purposes of direct marketing.
* To be informed about the mechanics of automated decision-taking process that will significantly affect them.
* To not have significant decisions that will affect them taken solely by automated process.
* To sue for compensation if they suffer damage by any contravention of data protection legislation.
* To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
* To request the supervisory authority to assess whether any provision of data protection legislation has been contravened.
* To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
* To object to any automated profiling that is occurring without consent.

## Appendix 3: 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) that use personal data. 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

The role and function of each of these subsidiaries is set out in the table below, along with an assessment of the data that is processed by the subsidiary and RNIB and their status in respect of who is the controller of the personal data. More detailed requirements for the sharing and processing of personal data are set out and defined in Intragroup Agreements entered into between RNIB and each subsidiary.

This policy applies to personal data that is processed by the RNIB subsidiaries.

**Table: Data protection roles and functions of RNIB subsidiaries.**

|  |  |  |
| --- | --- | --- |
|  | **Subsidiary role**  |  **RNIB role**  |
| **Shell charities** retained for legacy purposes:* Action
* BCNI
* Talking Newspapers
* National Library for the Blind
 | Receives legacy income – inc. names and addresses of executors etc. Joint controller  | RNIB processes legacy data on behalf of shell charities (which have no staff/ infrastructure of their own). Joint controller  |
| **RNIB Charity** ZA055845<https://ico.org.uk/ESDWebPages/Entry/ZA055845> | Operates the RNIB Establishments and holds data in respect of all regulated services. Joint controller Processor of data under contracts with Local Authorities etc.  | RNIB provides HR, database and IT support to RNIB Charity.Joint controller Sub-processor of Local Authority data.  |
| **RNIB Enterprises Limited**  | RNIB’s main trading company which undertakes the Transcription Services and runs the online shop.Joint controllerProcessor when undertaking transcription services for third parties. | RNIB provides HR, database and IT support to RNIB Enterprises.Joint controller Sub-processor in connection with transcription data |
| **RNIB Services Limited**Z5069026<https://ico.org.uk/ESDWebPages/Entry/Z5069026> | Collects school fees for Sunshine House.Joint controller Processor of data under funding arrangements.  | Provides finance support to RNIB Services Limited.Joint controllerSub-processor of funding arrangement data.  |
| **Lottery companies –**Rnib Direct Services Lottery LimitedZA459586<https://ico.org.uk/ESDWebPages/Entry/ZA459586>Rnib Feel Good Friday Lottery LimitedZA459583<https://ico.org.uk/ESDWebPages/Entry/ZA459583> | Operate the RNIB lottery and raffle Joint controller  | Provides HR, database and IT support to the companies which do not employ their own staff.Joint controller  |

## Version control

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author & Job Title | Status & Level of Approval | Changes |
| 5.0 | 21 May 2020 | IG Manager | Board Approval | Board approval following annual review and addition of section 2.12 |
| 5.1 | 13 May 2021 | IG Manager | Board approval | Board approval following annual review |
| 5.2 | 6 Sept 2021 | IG Manager | Director approval | Update role of SIRO |
| 6.0 | 18 May 2022 | IG Manager | Board approval | Board approved 30 June 2022 following annual review |

## Document control

The table has two columns and nine rows.

|  |  |
| --- | --- |
| **Document title** | Data Protection Policy |
| **Document owner** | Information Governance Manager (Data Protection Officer) |
| **Originally approved by** | Board of Trustees |
| **Originally approved on** | 30 June 2022 |
| **Approved by** | Board of Trustees |
| **Approved on** | 30 June 2022 |
| **Planned review date** | 31 May 2023 |
| **Is document published internally or on RNIB public-facing website?** | Internal and external |
| **Version no.** | 6.0 |

End of document