Policy Overview

Audience:	Operational	Category:	As Required
Doc Owner:	RCI DPO	Version No:	V2.0
Date Issued:	14 January 2025	Next Review:	16 January 2029

Version Control

Version No.	Review Date:	Update Notes:	Update By:
V1.0	7-Mar-23	New Policy.	RCI DPO
V2.0	14-Jan-25	Full review – Changes:	RCI DPO
		Ensuring clarity around the need for separate employee privacy notices and improving formatting for easier reading.	
	Click or tap to enter a date.	Choose an item.	

Contents

WHY IS THIS POLICY NEEDED

RCI Group Limited (RCI Group) and its subsidiaries are committed to ensuring compliance with all relevant and applicable laws, regulations, and legislations. We recognise and accept our responsibility to manage personal data in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and other legislation relevant to data protection and security.

The purpose of this policy is to support IG Leads and/or senior staff in understanding their responsibilities in relation to the development and implementation of privacy notices and to ensure a consistent, legally compliant, and transparent approach.

Privacy notices must exist for all stakeholders, including staff, customers, suppliers, and other relevant parties, to ensure transparency in how personal data is managed and processed in accordance with legal requirements.

WHO NEEDS TO READ THIS POLICY AND WHY

This policy applies to all staff responsible for the development, implementation and monitoring of RCI Group and subsidiary privacy statements, particularly Information Asset Owners, IG Leads and HR.

Information Asset Owners are responsible for ensuring that:

- IG Leads are made aware of new systems/processes that may affect their privacy notices
- RoPAs are updated with any new processing activities as necessary and reviewed regularly
- Staff complete their compulsory training, including information request training, according to their job role

IG Leads are responsible for:

- Up-to-date privacy statements are in place for their subsidiary for all stakeholders
- Staff have access to, read and understand RCI Group frameworks, policies and standard operating procedures (SOPs) as well as the individual subsidiary's policies and procedures, as applicable to the staff member's job role
- Developing and implementing Privacy Statements for their subsidiary
- Monitoring the implementation of their subsidiary's privacy statement
- Updating their privacy statement as and when necessary

The DPO is responsible for:

- Supporting IAOs and IG Leads: Providing guidance on privacy notices, RoPAs, and compliance with data protection laws.
- Auditing and Compliance: Regularly reviewing privacy notices and RoPAs to ensure accuracy and legal compliance.
- Monitoring and Advice: Supporting subsidiaries in developing, implementing, and updating privacy notices, and acting as a second point of contact for data protection queries, through the IG Leads.

THE PURPOSE OF A PRIVACY STATEMENT

The DPA 2018 and UK GDPR set out the legal framework for processing personal data. Providing accessible information to individuals about the use of their personal data is a key element of their legal right to transparency under the UK GDPR.

Data Controllers and Data Processors are responsible for providing this information and ensuring that individuals can access their information rights. RCI Group and its subsidiaries are classed as Data Controllers and may also be Data Processors, so they must inform staff, clients, patients, and other stakeholders about how their data is processed.

A privacy statement is the most common way to provide this information. It sets out the Data Controller's responsibilities, processes, and explains individuals' information rights and how to access them. RCI Policy requires privacy statements to be available on the website, so they remain easily accessible. They should also be included in induction packs and displayed on staff notice boards or intranets. Existing staff must be informed of the privacy statement and any updates or reviews made to it.

RCI Approach

RCI Group requires separate privacy notices for public stakeholders and for staff. The public notice must be published on the RCI Group website for easy access, with a reference or link to the staff notice. The staff notice must be shared during recruitment, at onboarding, and remain readily available internally, ensuring employees and applicants understand how their data is collected, stored, used, and shared. This approach maintains transparency and meets legal obligations by providing the right information to the right audience at the right time.

CONTENTS OF A PRIVACY NOTICE

Under the UK GDPR, a privacy notice must be:

- Concise, transparent, and written in plain, easily understood language.
- Clear and tailored to the understanding of the data subjects.
- Accurate and not misleading in any way.
- Freely available and easily accessible to individuals whose personal data is being collected, provided at the earliest opportunity.

It must contain:

Introduction and Organisation Details

A brief overview of the organisation, its functions, and its contact details.

Include the company/charity registration number and ICO registration number.

Data Controller and Processors

Identify the Data Controller and any relevant Data Processors.

If the organisation acts as both Controller and Processor, clarify which activities are controlled directly and which are delegated.

Data Categories

Specify the types of personal data collected/processed.

List the categories of data subjects (e.g., employees, clients, patients).

Purpose and Legal Basis for Processing

Describe why you are processing personal data and the lawful basis (e.g., consent, contract, legitimate interest, legal obligation).

Consent Provisions

Explain when and why consent is obtained, how it is collected (freely given, specific, informed, and unambiguous), and how individuals can withdraw it.

If another lawful basis applies, clarify that consent is not required.

Special Category Data

If you process special categories of data (e.g., race, religion, health), specify the condition under Article 9 of the UK GDPR that allows this.

Data Storage, Security, and Retention

Describe where data is stored, what security measures protect it, and how long it is retained.

Data Sharing

Explain which organisations or third parties receive data, why it is shared, and under what conditions.

Individual Rights

Outline the data subject's rights (e.g., access, rectification, erasure, restriction, objection, portability) and how to exercise them.

Contact Information

Provide the official RCI contact email address for the Data Protection Officer (RCI-DPO@rcigroup.co.uk) and the ICO for complaints or queries.

Security Measures

Summarise the technical and organisational measures that safeguard personal data.

International Transfers

If personal data is transferred outside the UK/EEA, specify how equivalent protection is ensured (e.g., Standard Contractual Clauses).

Changes and Reviews

Highlight how often the privacy notice is reviewed and how any changes will be communicated to data subjects.

Accessibility

Ensure the privacy notice is easy to find and access for all stakeholders.

Additional Considerations

If you collect personal data indirectly, explain how, from where, and why.

Include a summary of any automated decision-making or profiling, stating its logic and impact on individuals.

Cookies

Provide details about the use of cookies or similar technologies.

Explain when consent is required and how users can accept or reject non-essential cookies.

Essential Cookies Exception

Consent is not needed for cookies strictly necessary to provide an online service requested by the user.

ENSURING EFFECTIVENESS OF THIS POLICY

Compliance with this policy will be monitored by the RCI DPO via regular audits and this policy will be reviewed annually. The RCI DPO will report back to the RCI Board, via the RCI COO, who have overall responsibility for compliance with regulations and legislations within RCI Group Limited.

The aim of this policy is to ensure best practice and compliance with UK GDPR and Data protection Act 2018. Where these aims are not met or there is room for improvement, the RCI DPO will make recommendations to the RCI Board (via RCI COO) to improve compliance, agree upon actions and ensure that this is communicated to the subsidiary IG Lead.

The RCI DPO is responsible for updating this policy. The IG Lead is responsible for implementing this policy and any changes to it, within their subsidiary and communicating any changes to all staff within their subsidiary.

OTHER POLICIES AND PROCEDURES TO CONSIDER

This policy should be read in conjunction with:

- RCI Data Protection and Information Governance Assurance Policy
- RCI Group Information Requests Policy
- RCI Group Confidentiality and Data Protection Policy
- RCI Group Information Classification Policy
- RCI Group Information Lifecycle and Records Management Policy
- RCI Group Personal Data Breach Policy

Appendix 1: Equality Impact Assessment

Date of assessment:	14 January 2025
Completed by:	RCI DPO
Who is intended to benefit from the policy?	**Staff:** Ensures that all staff understand how their personal data is collected, stored, processed, and shared, thus promoting clarity, accountability, and consistency across the organisation. **Service users:** Ensures service users (such as customers, clients, commissioners) are aware of their data protection rights and how the organisation processes their data, thereby increasing trust and transparency**.**

Are there concerns that the policy could have an adverse impact because of:

	Yes / No	Rationale
Age	No	
Disability	No	
Gender	No	
Ethnicity	No	
Sexual orientation	No	
Religion / Belief	No	
Pregnancy / Maternity / Paternity	No	
Culture	No	

If the answer to any of the above is yes, consider the following:

	Tick	Rationale
Can it be demonstrated that such a disadvantage or advantage can be justified	☐	
Adjust the policy to minimise the disadvantage identified or better promote equality	☐	
If neither of the above is possible, submit to CQGC for review	☐	
		Choose an item.

Appendix 2: Definitions

For the purposes of data protection legislation, the terms ‘process’, ‘processed’ or ‘processing’ apply to any activity involving personal data, such as collecting, storing, sharing, using, destroying.

Data controller	The organisation who (either alone or in common with other people) determine the purpose for which, and the way data are processed.
Data Processor	A person or organisation who process data on behalf of and on the orders of a controller Data Subject – the person about who you are processing data.
Data Protection Officer	An officer of the establishment or local authority who is responsible for data protection issues within the organisation. The appointed RCI DPO
Data Subject	Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is an end user whose personal data can be collected.
Personal Data	Any information which on its own or in conjunction with other information available, can identify a Data Subject. This includes any records containing information about a data subject
Special Category Data	Certain types of personal data are classified as special category data under UK GDPR. If you control or process this data, you must have an additional lawful basis for processing it, in line with the regulations. Special category data includes information about: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Health • Biometric data (when used for identification purposes) • Genetic data • Sexual orientation • Sex life
Criminal Offence Data	Any personal data which is linked to criminal offences, or which is specifically used to learn something about an individual's criminal record or behaviour. Data relating to criminal offences is also afforded similar special protection.
Stakeholders	Any person with an interest in RCI Group and its subsidiaries

Appendix 3: Example List of Categories

The following are examples of categories that subsidiaries should tailor to their specific needs and include within their privacy statements. Each subsidiary should identify their own stakeholders, data categories, purposes, and lawful bases relevant to their processing activities.

Stakeholders	Data Categories	Purpose for using data	How data is collected	Lawful basis	Who is data shared with and why
Employees	Basic personal details	Employment	Requested by us	Consent	Law enforcement
Job Applicants	Contact details	Service/Care/Support provision	Freely provided	Contract	Third Party Care providers
Patients	Next of kin details	Contract	Contacting us	Legal Obligation	Third party systems
Service Users	Test results	Continuity of care	Shared by other care service/provider	Vital Interest	Third Party professionals
Clients	Feedback	Security/Vetting applications		Public Task	Courts
Contractors, Third Party Providers and Suppliers	Information about referrals	Ensuring compliance		Legitimate Interest	With staff and within the business only
Business Contacts	Medical records/history	Exchanging services			

Key Notes:

This is a general guide. Each subsidiary should ensure their categories align with their processing activities and ensure transparency in their privacy statements.

Special Category Conditions - Whenever processing special category data (e.g., health, race, or sexual orientation), a specific condition under Article 9(2) of the UK GDPR must be met, and this should be stated explicitly.

Criminal Offence Data - The processing of criminal record information requires meeting conditions under Schedule 1 of the Data Protection Act 2018.

Processor Responsibilities - If you are acting as a Data Processor, you process data on behalf of the Data Controller and do not establish the lawful basis for processing. It is the responsibility of the Data Controller to determine the lawful basis and inform data subjects accordingly.

Appendix 4: Cookie Banner Checklist

A guide to setting up a cookie banner:

- Include a button to accept or reject cookies. The cookie banner must have a button to allow the user to accept cookies. The text in the cookie banner and the button must make it clear that by clicking the button the user agrees to the deployment of cookies.
- Should mention that “agree” and “reject” boxes should be the same size and font and should be placed side by side rather than in a position where the “accept” button would be more noticeable.
- Include a button to let users manage optional and non- essential cookies.
- Provide detailed information about cookie use and essential cookies. According to UK GDPR, websites need to provide enough information to the user about their cookies use so they can make an informed choice about whether to accept cookies. The cookie banner should contain information about why the website uses cookies. For example, does it collect data for analytics, advertising, or social media purposes?
- Alert the User if the Website Shares Data with Third Parties. If the website shares the data collected through cookies with third parties, for example, advertising or analytics partners, the cookie banner should explain this to the user. Additionally, many websites choose to link to a list of vendors they share this data with on the cookie banner.
- Link to the Website’s Cookie Policy. The cookie banner should contain a link to the website’s cookie policy (or cookie notice). Here the website will provide further information about the cookies in use on the site, including a list of all the cookies.
- Include a Link to the Cookie Settings. Many websites that comply with the GDPR include a link to its cookie settings page on the cookie banner. This isn’t required under GDPR as long as users have the choice to reject all cookies. However, it does have the benefit of allowing users who would otherwise reject all cookies to permit some forms of data collection. For example, a user could reject cookies used for targeted advertising, but accept cookies used for website analytics.
- Pre-ticked boxes also aren’t allowed. The guidelines go as far as to advise websites not to nudge users towards accepting consent, for example by emphasising “agree” over “reject.”

Commented [JB1]: Should mention that “agree” and “reject” boxes should be the same size and font and should be placed side by side rather than in a position where the “accept” button would be more noticeable.