Respond Privacy Policy

Version: Version 2
Review Date: 03/09/2024
Next Review Date: 03/09/2026
Department Owner: Head of Compliance & Quality Assurance
Department Expert: Compliance and Data Protection Analyst

Table of Contents

Version Control 3

Review and Approval Process 3

Ownership 3

1.0 INTRODUCTION 4

2.0 PURPOSE OF THE POLICY 4

3.0 SCOPE OF POLICY 5

4.0 OBJECTIVES OF POLICY 5

5.0 ROLES & RESPONSIBILITIES 5

6.0 POLICY IMPIEMENTATION 6

7.0 CUSTOMER CARE 17

8.0 POLICY REVIEW 17

9.0 POLICY SCHEDULE 17

10.0 IMPACTED DEPARTMENTS 18

11.0 REPORTING MONITORING AND KPI'S 18

12.0 RELATED POLICIES 18

13.0 REFERENCE 19

Version Control

Policy Expert Author	Version	Reviewed By	Date of Review/Approval
Michael Dignam	1.0	Nessa Aylmer	27.06.2022
	1.0	EMT	30.06.2022
	1.2	FRAC	12.07.2022
	1.3	Board	26.07.2022
Valerie Kirwan	2	FRAC	20.08.2024
		EMT	22.08.2024
		Board	03.09.2024

Review and Approval Process

This policy will be reviewed every 2 years

Ownership

The owner of this policy is the Executive Head of Compliance & Quality Assurance.

1.0 INTRODUCTION

At Respond, we are committed to protecting and respecting your privacy. This privacy policy explains how Respond collects, handles, shares, protects and uses all personal information and individual rights in relation to that information. Under the General Data Protection Regulation (GDPR) of May 2018 and all other applicable laws, Respond is the controller of that information and takes your privacy seriously and is dedicated to safeguarding your personal data while ensuring transparency in how we manage it.

The policy details why and how we will use personal information that we have obtained from tenants, service users, employees and Others whom we share it with and the rights in connection with the information we use. It also sets out data subject rights that assist in controlling your privacy and managing your information.

2.0 PURPOSE OF THE POLICY

This purpose of this policy is to inform you about how Respond collects, uses and manages your personal data. Our Privacy Policy helps demonstrate compliance with data protection law, in particular in respect of our obligations under the transparency principle (Articles 12 to 14 of the General Data Protection Regulation (GDPR).

We will set out the way we handle and use the personal information that we obtain from all the different interactions you may have with us as a business or as an employee, committee or board member. This will include but is not limited to any interaction from tenants, service users and other, social media platforms or our website when you contact us.

Respond is the Data Controller in relation to processing personal information as set out throughout this policy. This means that Respond

decides why and how your personal information is processed. Please see section 5 for the relevant contact and legal information.

3.0 SCOPE OF POLICY

The scope of this policy applies to all areas of the organisation, to all of its Board and subcommittees, employees and any areas of operational activity involved in the handling of personal information including but not limited to housing delivery, landlord / tenant relations, and any setting where supports and/or services are provided and when engaging with external stakeholders, contractors, suppliers or any other body or parties in their daily operational activities.

4.0 OBJECTIVES OF POLICY

Respond at all times aims to ensure that all of its Board, subcommittees and employees, HR department are aware of their obligations to proactively and effectively manage and process all personal information we store, obtain and process from our Tenants, Service Users, Employees and Others in line with the GDPR and all other Data Protection legislation. Respond strives to ensure that all personal data is handled lawfully, fairly and transparently and at all times to uphold the rights of individuals.

5.0 ROLES & RESPONSIBILITIES

Throughout this document, “we”, “us”, “our” and “ours” refer to Respond. Respond is a registered charity, a company limited by guarantee and registered at the following address: Airmount, Dominick Place, Co Waterford, Ireland.

All staff are trained and updated regularly on Data Protection matters and are required to comply with this policy.

The appointed Data Protection Officer is responsible for overseeing questions in relation to this privacy policy, if you have any questions or should you want to exercise your legal rights under General Data Protection Regulation (“GDPR”), please contact the Data Protection Officer using the details set our below.
Email address: data.protection@respond.ie

Postal address: Data Protection Officer, High Park Campus, Grace Park Road, Drumcondra, Dublin 9

6.0 POLICY IMPEMENTATION

Respond has established procedures and guidelines to ensure that personal data is collected, processed and stored in accordance with the General Data Protection Regulation.

6.1 What information do we collect (?)

We collect Personal information about Tenants/Service Users/Employees/Others

We receive personal information about you that you give to us, that we collect from your visits to website, and social media pages and that we obtain from other sources. We only collect personal information which we need and that is relevant for the purposes for which we intend to use it.

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where their identity has been removed (anonymous data). We may collect, use, store and transfer different kinds of personal data (also includes special categories of sensitive data (Article 9 GDPR) about you which we have grouped together as follows:

Data Type	Data Includes the following
Identifying Data	First name, last name, username or similar identifier, title, date of birth and gender.
Contact Data	Postal address/Eircode, email address and telephone contact numbers.
Technical Data	Internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform along with other technology that you use on the device(s) you use to access this website.
Usage Data	Information on how you use our website and the

	services we offer.
Marketing and Communications Data	Includes your preferences in receiving marketing from us and your communication preferences, tenancy and/or service user details, gender and historical transactions.
Tenancy and Service User Details	We may collect information in relation to your tenancy/service you use with us, location and tenancy /service user communication/transactions.
Transaction Data	Includes data such as payment transactions or tenancy term.
Financial Data	Detailed financial information including contact details, income details, marital status, date of birth, gender, residential status, employment details, linked relationships, bank details and payment method.
Interaction Data	Information about your interactions with us, including correspondence and phone calls and text messages between us and you.

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate our usage data to calculate the percentage of users accessing a specific website feature.

However, if we combine or connect the Aggregated Data with your personal data so that it can identify you directly or indirectly, we will treat the combined data as personal data which will be used in accordance with this privacy notice. We may also anonymise data so that it is no longer personal data.

Our website is powered by Originate, our third party web services provider. We ensure all third party providers share our commitment to ensuring that all data is processed in accordance with applicable data privacy laws and is kept secure.

When our website is visited by you, the web management service collects standard internet log information (your internet domain, your IP address, browser, and type of device) and details of behaviour patterns (where you joined there site from, the path you take through our site and where you leave, the pages visited and the documents downloaded), these are stored against unique ids (which are a sequence of numbers).

This data is collected for legitimate business purpose of monitoring the number of visitors to the various parts of the website, the general geographic location of visitors and engagement levels, Google analytics may also be used by the web management service to collect standard internet log information and details of visitor behaviour patterns which in turn enables improvements to be made to the service we offer and accessibility to our website, also providing business intelligence. This information is only processed in a way which does not identify anyone. This data is kept for an indefinite period of time.

6.2 Use of your personal information/How do we use your personal information (?)

We use your personal information for a variety of reasons. We rely on different legal grounds to process your personal information, depending on the purposes of our use and the risks to your privacy. You will only receive emails from us if:

- Where we need to implement the contract, that you have entered into or are about to enter into to.
- Where it is necessary for our legitimate interests (for those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.
- Where we rely on the consent to process your personal data. You have the right to withdraw to consent at any time. If you are making an enquiry with us through our website, by phone or in person in any of our service locations.

What is our legal basis for processing your information (?)

Article 6 of the General Data Protection Regulation (GDPR) sets out the legal bases for Processing Data. Processing of personal data is only lawful where it has a 'legal basis'.

Respond, as a data controller, has to determine a legal basis to rely on in order to ensure that any processing undertaken is lawful. The principle of lawfulness, fairness, and transparency are of particular relevance to the question of legal basis.

The basis for processing personal data is closely tied to the purpose of the processing, and the principle of purpose limitation plays an important role in ensuring that processing has a valid legal basis. Personal data will only be collected by Respond for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Respond endeavor to be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The Organisation will at all times be cognizant of Article 5 principle of **'**data minimisation' , which requires that personal data be "adequate, relevant and only limited to what is necessary and only collect data in line with these principles.

The legal bases for processing data include-

Consent- data subject has given their consent to the processing of their data
Contract- which the data subject is party to
Legal obligation- processing is necessary for compliance with a legal obligation to which the controller is subject
Vital interests- processing is necessary in order to protect the vital interests of the data subject or of another natural person
Public task- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
Legitimate interests- processing is necessary for the purposes of the legitimate

interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Respond obtain consent where it is required and generally relies on having a legitimate interest to process the data in most other circumstances.

The reasons why we may process your personal data are set out below:

Activity	Type of Data	Lawful basis
To process and provide you with a tenancy agreement or a quotation for any service we provide	• Identity • Contact information • Financial	Contractual obligation
Register as a service user/tenant	• Identity • Contact information	Contractual obligation
Family Support Services	• Identity, • Health Special Categories of Data	Legitimate Interest Vital Interests of Data Subject.
Child Protection	• Identity • Special Categories of Data	Legal Obligation
Register with the RTB, POBAL, PASS, ECCE, HSE, Tusla	• Identity • Contact information	To comply with legal and regulatory obligations

Insights and surveys	• Identity • Contact information • Service location	Legitimate interest (engagement and service improvement)
General business needs: • Accounting • Administrative purposes	• Identity • Contact information • Financial	Legitimate interest
To deliver relevant website content	• Identity • Contact • Profile • Communication • Technical • Usage	Legitimate interest (to develop and grow our organisation)
Data analytics on our website	• Usage • Technical	Legitimate interest (to keep website relevant and updated to define our customers and the services they need)
To administer and protect our business (troubleshooting, system maintenance and support)	• Identity • Contact • Technical	Necessary for our legitimate interests (for providing a relevant service, for administration, IT security, business reorganisation or restructuring)

To provide you with service communications by post, text and/or email.	• Identity	We only communicate with current service users under legitimate interest, for potential service users we will only provide information to you upon consent. You may withdraw this consent at any time.
Legal Obligations	• All personal data we collect	We may process your personal data to fulfil legal obligations such as complying with GDPR, anti-money laundering obligations, etc.

CCTV use

All relevant premises are also monitored by CCTV camera for security purposes. We have strict retention policies in respect of CCTV footage and process data captured by CCTV for security purposes in our legitimate interest. CCTV is only deployed when it is necessary and proportionate to do so.

All external phone calls through our Customer Services Centre are recorded, we will use this information to monitor and train staff and to deal with customer disputes. Recordings of calls are subject to strict retention periods

6.3 Records of Processing Activities (RoPAs)

Respond, in line with Art. 30 of the GDPR will maintain comprehensive records

of all processing activities under its responsibility. These records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. Respond will ensure that all records of processing activities are regularly reviewed and updated to reflect any changes. These records are recorded on the Privacy Engine system by all data champions and available for inspection to the relevant authorities upon request.

6.4 Changes to the privacy policy and your duty to inform us of change

Any changes we make to this privacy policy in the future will be posted on our Respond website. Please check back frequently to see any updates for changes to this privacy policy. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

6.5 Third party links

Our website may include links to third-party websites, plugins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not have any control over third party websites and are not responsible for their privacy policies. When you leave our website we encourage you to read the privacy policy of every website you visit.

6.6 If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide the data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example , provide you with the service you require). In this case, we may have to cancel the service you have with us but we will notify you of this at the time.

6.7 Promotional offers from us

Occasionally we may engage in a promotional activity, this is to highlight parts of our service or for charitable purposes. We will only offer this to individuals engaged in our service and have consented, you may withdraw this consent at any time.

6.8 Opting out

You can request us to stop sending promotional offers to you at any time by emailing your wishes to data.protection@respond.ie. But this will not apply to personal data provided to use as a result of a contract or regulatory requirements, service experience or any other transactions acquired for general business purposes as noted in the table above.

6.9 Cookies

You can set your own browser to refuse all or some browser cookies, or to alert you when websites set or access cookies, if you disable or refuse cookies, please note that some parts or this website may be inaccessible or not function to its full capability.

6.10 Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use if for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the process for the new purpose is compatible with the original purpose, please contact us by using the below link
Contact Us - Respond

If we need to use your data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent. In compliance with the above rules, where this is required and/or permitted by law.

6.11 Transfers outside of the EEA

We generally do not share your information with any organisation outside of the European Economic Area ("EEA"). Sometimes IT Application service provider's servers are located in the USA or outside the EEA and are therefore subject to their own privacy law or they may not have adequate data protection laws equivalent to those in the EEA. If your personal data needs to be transferred to and processed in countries outside of the EEA, we will ensure that appropriate technical and organisational safeguards are in place to protect your data in compliance with GDPR, we will only send the personal information to USA entities subject to Standard Contractual Clauses approved by the European Commission or where we have an alternative

safeguard in place in accordance with applicable law. Where they apply to our data transfer activities, we may rely on adequacy decisions from the European Commission about certain countries for data transfers to countries outside the EEA.

6.12 Disclosure of your information

We may share your personal information with third party service providers that perform services or functions on our behalf such as the following:

- Accountants.
- Solicitors
- Consultants.
- Business advisors.
- IT service providers.
- Printers.
- Communications companies who may carry our awareness campaigns on our behalf.
- Providers of security services.
- Administrative services, etc..
- Local Authorities.
- Contractors.
- Government Departments and State/Semi-State Bodies.
- Residential Tenancies Board.
- An Garda Siochana.
- The Criminal Assets Bureau.
- Tusla.
- Pobal.
- DRHE.
- HSE.
- HSA.
- HIQA.
- Revenue Commissioners.
- Agents.
- Funders etc..

Data sharing agreements are also executed where applicable between Respond and the 3rd party recipient of the personal data to further safeguard your privacy rights.

6.13 How long will we retain your personal data for?

We will only retain your personal data and records for as long as necessary to fulfil the purpose we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements in line with Respond's data retention schedule as set out in the Data Retention and Destruction Policy.

6.14 Your legal rights

You have a number of rights under data protection law in relation to how we use your personal information. You have the right, free of charge, to:

1. Right of Access by the Data Subject to check what type of personal data we hold about you and what we do with that information. You are also entitled to receive a copy of this information.
2. Right to Rectification and to have any inaccurate personal data which we hold about you updated or corrected.
3. Right to Erasure of personal information we hold about you, upon request.
4. Right to Restriction of processing and to stop us from using your personal information in certain cases, including if you believe that the personal information we hold about you is inaccurate or the use of the information is unlawful, if you exercise this right, we will store your personal information and will not carry out any other processing until a resolution is found.
5. Right to object to us using your personal information where we rely of our legitimate interest to use your information. We will stop using your personal information unless we can demonstrate overriding legitimate grounds for the continued processing of this information.
6. Withdrawing consent, where you disagree how your personal information is processed. You can withdraw consent at any time by emailing data.protection@respond.ie
7. Right to Data Portability and to receive certain aspects of your personal information in a structured, commonly used and machine readable format and to have that information transferred to you or another data controller.
8. Right to not be subject to a decision based on automated processing
9. Right to complain, you have the right to complain to the Data Protection Commissioner, details on link provided below.

Please note these rights are in some circumstances limited by the data protection legislation. If you wish to exercise any of these rights please contact us using the contact details mentioned above. We will endeavor to respond to your request within one month. In the unlikely event we are unable to deal with your request within this time frame we may extend this period by a further two months and will explain why.

You also have the right to lodge a complaint to the office of the Data Protection Commission. Please use the below link should you wish to make contact:
How to contact us | Data Protection Commissioner

Should you require further information on data protection you may also visit www.dataprotection.ie

6.15 Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process any personal data on our instruction and they are subject to a duty of confidentiality.

Our security practices include the use of encryption, secure servers, firewalls, and access controls, ensuring that only authorised personnel have access to personal data. We also conduct regular cybersecurity testing and assessments to identify and address potential vulnerabilities. In the event of a data breach, we have established protocols to respond promptly and effectively, including notifying affected individuals and relevant authorities as required by law. Our commitment to data security is central to maintaining the trust and confidence of our donors, volunteers, beneficiaries, and all those who engage with our Organisation.

We have also put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of any breach where we are legally required to do so.

7.0 CUSTOMER CARE

Respond will at all times endeavour to proactively and effectively manage and process all personal information we store, obtain and process from our Tenants, Service Users, employees and Others in line with the GDPR and ensure that all of its Board, subcommittees and employees are fully aware of their obligations in this regard. Respond also endeavour to keep Tenants, Services Users, Employees and others fully up to date of any changes to this policy in a timely manner.

8.0 POLICY REVIEW

This Policy will be reviewed every two years or will be amended to take account of any external regulatory changes, external market changes or internal organisational change as necessary. All policies are presented to the relevant Respond Sub Committees for consideration and review prior to being recommended to the Board for approval.

9.0 POLICY SCHEDULE

A policy schedule is maintained by the Head of Compliance with input from all of the Heads of Department. It includes the owner's names, dates for review and versions of documents held as current and operational within Respond. This schedule is presented to the Community, Support, Research and Advocacy (CSRA) Committee and the Finance Risk and Audit Committee (FRAC) for review on a regular basis.

The current schedule is available on

X:\Policies and Procedures\Policy Schedule\Respond Global Policy Schedule

File Name is Respond Global Policy Schedule updated 16-02-2022

10.0 IMPACTED DEPARTMENTS

All departments are impacted by this policy.

11.0 REPORTING MONITORING AND KPI'S

- All board and staff members to be fully trained on this policy through Privacy Engine.
- All breaches of this policy to be recorded in the Respond Risk Incident Management Portal.
- Contracts/Application forms/website/employee manual contain privacy notices and are regularly reviewed and updated.
- Express Consent is obtained from a data subject only where Respond cannot rely on other lawful basis's for processing.
- Data processing and data sharing agreements with third parties are entered into where applicable.
- All records of processing activities (RoPAs) to be updated as required and recorded on Privacy Engine
- All personal information that we store and process to be only retained for as long as Respond have a lawful basis for doing so.

12.0 RELATED POLICIES

- Data Protection Policy.
- Data Protection Impact Assessment Policy.
- Data Breach Policy.
- Data Subject Rights Access Policy.
- Confidentiality Policy.
- CCTV Management Policy.
- Data Retention and Destruction Policy.

13.0 REFERENCE

This policy should also be read in conjunction with

- General Data Protection Regulation (GDPR) 2018.
- Data Protection Act 2018.
- Data Protection Act 1988, 2003.
- CCTV Guidance For Data Controllers, Data Commission, May 2019.
- ePrivacy Regulations 2011.
- Data Protection Commission Guidance on Legal Bases for Processing

Personal Data.