Privacy and data protection statement – research projects

Acuity Research & Practice Ltd is committed to protecting your privacy.

Acuity carries out research on behalf of our clients in order to help them improve services and engage with their residents. Clients provide us with personal data such as names and addresses to enable us to carry out this research.

This policy explains how the data provided to us by our clients and the data we collect as part of our research is protected by Data Protection Legislation. Acuity also has a **General Privacy and Data Protection Statement** that can be found on our website https://www.arap.co.uk/who-we-are/#policies

1 Research objectives

The specific purposes of each research project will be clearly explained to participants. Depending on the nature of the project, purposes may include:

- To explore residents' satisfaction with their home and the services provided by their landlord
- To investigate which issues are most important to residents
- To measure satisfaction levels against the importance of issues
- To identify any new issues the landlord may not be aware of
- To feed back the results of the survey to enable the landlord to improve the services it provides
- To provide feedback to residents
- To monitor the performance of contractors
- To update resident details

2 Acuity commitment to research participants

The identities of research participants and their responses will be treated confidentially and used only for the purposes explained to them, unless the participant has expressly agreed to disclosure or disclosure is otherwise required or permitted by law.

We will not mislead you.

Co-operation is voluntary at all times. Personal information will not be sought from you or about you, without your prior knowledge and agreement.

Withdrawal – at any stage you can refuse to answer specific questions. You may decline to answer any question or withdraw from the research at any stage. You may also ask for some or all of your responses to be deleted. Where Acuity is acting as Processor, such requests will be handled in accordance with the Client's instructions and applicable Data Protection Legislation

We will not send unsolicited mail or pass on your data to others for this purpose.

If you have any further questions please contact us through the

https://www.arap.co.uk/#contact

You are welcome to check our credentials by contacting your landlord.

3 Data Protection Legislation

3.1 Interpretation

“Data Protection Legislation” means all applicable UK data protection and privacy legislation in force from time to time, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and any applicable amendments, replacement legislation, regulatory requirements, guidance and codes of practice issued by the Information Commissioner’s Office (ICO). Where EU GDPR applies to particular processing activities, Acuity will also comply with the applicable requirements Where personal data is transferred internationally, Acuity will ensure that appropriate safeguards and transfer mechanisms are in place in accordance with applicable Data Protection Legislation.

“Data Subject”, “Personal Data Breach”, and “Data Protection Officer” take the meaning given in the Data Protection Legislation.

“Data Controller” - A person or organisation that determines the purposes and means of processing personal data.

“Data Processor” - A person or organisation that processes personal data on behalf of a Controller.

“Personal Data” - Any information relating to an identified or identifiable living individual.

“Personal Customer Data” - Personal data relating to the Client's customers or residents that is processed in connection with a research project

“Sub-contractor” - A sub-contractor is any individual or organisation contracted to undertake part of a project.

3.2 Responsibilities

For research projects where the Client determines the purposes and means of processing and Acuity processes personal data solely on the Client's documented instructions, the Client will act as Controller and Acuity will act as Processor. The respective data protection roles and responsibilities will be confirmed within the applicable contract or data processing agreement.

Acuity undertakes to process and store data in accordance with the Data Protection Legislation, the requirements of the MRS Code of Conduct and in compliance with the ISO20252:2019 and ISO9001/27001 standards.

The Client will ensure that any personal data used for this project will have been processed in accordance with the Data Protection Legislation.

This contract will be reviewed with any change in relevant Data Protection Legislation and any necessary amendments will be agreed in writing and appended to this contract.

3.3 Data Sharing

Where personal customer data is passed to Acuity, The Client will ensure that the data has been collected with appropriate data protection notifications to customers, including consent where appropriate, to enable data to be transferred to Acuity to conduct activities on The Client behalf.

Personal customer data provided by The Client will be limited to data that is required for the specific project to be conducted by Acuity and will not include any other personal data.

3.4 Data Transfer and Storage

The Client data including personal data and/or personal customer data will be transferred to and from Acuity by secure and encrypted means as appropriate for the type and sensitivity of the data.

Acuity will take reasonable steps as appropriate for the type and sensitivity of the data to keep the data secure and will ensure confidentiality for all employees, workers, temporary workers, agency staff, sub- contractors working on this project.

Acuity will take appropriate technical, operational and security measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Acuity uses approved systems and service providers to collect, process and store research data. Appropriate technical and organisational security measures are applied based on the nature and sensitivity of the information processed. These include appropriate access controls, authentication, encryption and secure methods of data transfer and storage.

Access to personal data is restricted to authorised personnel who require access for legitimate business purposes. Acuity reviews the security and suitability of systems and relevant suppliers as part of its information security and supplier management processes.

Acuity will not disclose identifiable research responses to the Client unless the participant has been informed of and, where required, consented to the disclosure, except where disclosure is required or permitted by law.

When Acuity transfers personal data to The Client, in whatever form (e.g. digital, paper, recordings), the data will only be used for the purpose stated at the time it was collected. For this project this will be for research purposes and to ensure that The Client is meeting its responsibilities to their residents.

Acuity will not make a restricted international transfer of personal data except in accordance with the Client's documented instructions and applicable Data Protection Legislation. Where such transfers occur, appropriate safeguards and transfer mechanisms will be implemented as required.

3.5 Data Collection

When Acuity collects any information and/or personal data on The Clients behalf it will do so for purposes consistent with the proper performance of the contract.

When Acuity collects any personal data for this project it will do so as a Data Processor as agreed with The Client.

Acuity will be responsible for

- Processing data only in line with the terms of this agreement and the project scope.

- Acting only on written instruction from the Controller unless required to do so by law. The Processor is expected to inform the Client of any requirements on it to act outside of this contract in advance of undertaking the action unless they are legally unable to do so for reasons of important public interest.
- Ensuring that all people processing the data are subject to a duty of confidence.
- Taking any appropriate technical and organisational measures to ensure the security of the processing.
- Taking into account the nature of the processing and the information available to Acuity, assisting the Client where reasonably required with its obligations relating to data protection impact assessments, security of processing and personal data breaches.
- The Processor must assist the Controller in meeting its obligations under subject access requests; the Controller should be notified in writing of any subject access request made to the Processor as soon as possible to allow the Controller to direct the Processor as necessary.
- The Processor must notify the Controller of a potential or confirmed data breach in writing within 24 hours.
- The processor shall submit to audits and inspections and to provide the Controller with any information needed to ensure it meets its obligations to data protection.
- Engaging sub-processors only with the Client's prior specific or general written authorisation and ensuring that appropriate written contractual terms are in place requiring the sub-processor to provide an equivalent level of protection for personal data.

3.6 Data minimization and privacy by design

Acuity will only collect and process personal data that is necessary and proportionate for the specified research purpose. Data protection and information security requirements will be considered when research projects, questionnaires, data collection processes and reporting arrangements are designed. Where proposed processing is likely to result in a high risk to individuals, Acuity will assist the Client with the completion of an appropriate Data Protection Impact Assessment where required.

3.7 Data Retention

Unless otherwise agreed with the Client, personal data relating to a research project will normally be retained for up to 365 days following completion of the project. The applicable retention period will be documented within the project specification or other agreed project documentation. Different retention periods may be agreed with the Client where appropriate.

Paper copies of survey responses are kept for up to 6 months or as agreed with the Client and any call recordings are held for 90 days.

Acuity will ensure that any sub-contractors used for the completion of the project will retain data in accordance with agreed requirements in-line with this contract or specific written instructions of the Client.

NB: Anonymous satisfaction findings are not personal data and can be retained for the purposes of research, benchmarking and tracking over time

3.8 Data Deletion and Destruction

Acuity will delete and destroy data by means as appropriate for the type and sensitivity of the data. All paper documents including questionnaires are securely destroyed with full documentation. Acuity uses Microsoft 365 to store data in a secure environment. We use a

file structure to ensure that all personal and sensitive data that we store is kept in a distinct area of the file system so it can easily be identified and deleted when it is no longer needed at the end of the agreed retention period. Data deletion dates are diarised at the start of any project. Personal data will be securely deleted, anonymised or otherwise disposed of in accordance with Acuity's data retention and disposal procedures and the Client's documented instructions. Acuity survey and dashboard applications are fully compliant with GDPR; no personal data is stored if it is not essential and the applications include functionality to delete all personal data when it is no longer required for the project, or if an individual requests the right to be forgotten.

Acuity will ensure that any sub-contractors used for the completion of the project will delete and destroy data in accordance with agreed requirements in line with this contract or specific written instructions of the Client.

At the end of the provision of services, Acuity will, at the Client's choice, securely delete or return personal data processed on the Client's behalf, unless applicable law requires that the data is retained.

3.9 Notification

Acuity shall notify the Client immediately if it:

- receives a Data Subject Access Request (or purported Data Subject Access Request)
- receives a request to rectify, block or erase any Personal Data;
- receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- becomes aware of a Data Loss Event

Taking into account the nature of the processing, Acuity shall provide the Client with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made.

Document version:

Version: Privacy And Data Protection Statement - Research Projects 2026_v2.Docx
Last Reviewed: 21 October 2026
Next Review: 31 December 2026