POLICY

Data Protection and Information Security Policy

1. Introduction

This Policy sets out how Citizen will ensure its meets not only its legal and regulatory obligations, but its commitment to accountability and transparency for its customers, employees, and Board Members in the processing of their personal information. It ensures that Citizen complies with the UK General Data Protection Regulation (UK GDPR) and, the Data Protection Act 2018.

This Policy relates to the way information is gathered, managed, accessed, transmitted and operated from a Data Protection and Information Security perspective. This Policy's objectives are to:

- Ensure compliance with the UK GDPR and Data Protection Act 2018
- Ensure compliance with the Privacy and Electronic Communications Regulations (PECR)
- Protect Citizen's Information Assets (hardware, software, electronic data and hardcopy information)
- Maintain our registration with the Information Commissioner's Office
- Ensure compliance with recognised good practice
- Maintain information security for business reasons
- Minimise the risk of a personal data or information security breach
- Assist in the prevention, detection and management of security incidents
- Ensure the right balance between tight security and adequate access

The Data Protection and Information Security Policy aims to ensure:

Relevance of information – ensuring we collect sufficient information for a specified and lawful purpose

Confidentiality of information – ensuring that information is accessible only to those authorised to have access

Integrity of information – safeguarding the accuracy and completeness of information and processing methods

Availability of information – ensuring that authorised users have access to information and associated assets when required

Regulatory compliance – ensuring that Citizen meets its regulatory and legislative requirements

2. Scope

This Policy applies to:

- All areas of the business, including all users of Citizen information systems
- All data systems whether maintained on paper or in electronic format
- Citizen owned computing devices and privately owned devices which are used to communicate with the Citizen data network
- Communication lines and all associated equipment or devices used on Citizen premises or connected to Citizen resources that are capable of processing or storing Citizen's information.
- All staff, contractors and suppliers operating on our behalf.

The legal obligations placed upon Citizen and its staff and wide ranging and if breached could impact Citizen's ability to deliver services which respect customer confidentiality and ensure integrity and availability of customer personal data.

The key obligations for all staff, contractors and suppliers:

- Comply with the requirements of UK GDPR and Data Protection Act 2018 and its seven principles (see page 5).
- Ensure processing of personal data complies with Citizen's Privacy Notices located at https://www.citizenhousing.org.uk/privacy/
- Use only the minimum necessary (see the Citizen Data Rules for guidance on minimum, relevant, appropriate, excessive and necessary use of personal data) personal data relevant to the purpose for which it was obtained.
- Do not use personal data for a different purpose to which it was originally collected.
- Do not introduce unauthorised software (software requires ICT authorisation see the ICT Acceptable Use and Data Protection Standards) into Citizen; it may have an impact on confidentiality, integrity and availability of personal data.

3. Policy detail

3.1 Definitions

All staff need to be familiar with the following definitions:

Data Subject: an identified or identifiable living person who can be identified, directly or indirectly, in particular by reference to an identifier.

Personal Data: any information relating to a Data Subject such as an identifier including a name, an identification number, location data (a customer address is personal data on its own), 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 means 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;

Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a living individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Data Controller is an organisation or sole trader which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor is an organisation or sole trader which processes personal data on behalf of the Data Controller;

3.2 Policy Principles

- Ensure that Citizen has an Information Security Management System (ISMS) that supports the principles and requirements of UK GDPR and DPA 2018;
- The ISMS provides a regime that ensures through robust standard operating procedures the appropriate monitoring and auditing of compliance with this Policy;
- The ISMS ensures through its comprehensive and robust nature that confidentiality, integrity and availability of Citizen's information systems;
- The ISMS ensures that the fundamental requirements of the legislation are constantly reviewed such as the need for data protection by design and that appropriate security measures and controls are in place to balance need for confidentiality, integrity and availability.

3.3 Procedural Safeguards

- Ensure that all employees, contractors and suppliers as necessary are aware of our Policy and procedures.
- Undertake auditing, monitoring and risk assessments including Data Protection Impact Assessments, Bias audits and Legitimate Interest Assessments as appropriate.
- Comply with standard operating procedures to ensure the rights of data subjects are respected including but not limited to the right of data subject access.
- Provide regular monthly updates to the Information Steering Group in respect of performance KPI's.
- The Policy will be reviewed annually and will be influenced by changes in legislation and guidance issued by the Regulator (Information Commissioner's Office).

3.4 Employee expectations

- Ensure that all colleagues have appropriate training and recourse to advice and guidance in relation to this Policy.
- Provide all colleagues with on-line e-learning to ensure an appropriate level of training.
- Provide class-room style training and workshops to suit the learning needs of colleagues and offer re-training in appropriate circumstances.

3.5 Listening to colleagues and customers

The provision of service under this Policy is heavily influenced by the requirements and needs of all data subjects aligned with the need to comply with the UK GDPR and DPA 2018, first principle that requires transparent, fair and lawful processing of personal data. Furthermore, the legislation upholds the rights of all individuals in respect of the processing of special categories data often associated with the protected characteristics specified in the Equality Act 2010.

3.6 Data Protection, UK GDPR and PECR

Citizen employees and contractors will read and work by the terms of this Policy and act in line with the requirements of UK GDPR and the Data Protection Act 2018 and its seven principles. These state that Personal Data should be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures," and
- Accountability requires Citizen and all staff take responsibility for handling personal data in line with the requirements of the six other principles. Citizen must have appropriate measures and records in place to demonstrate compliance. Citizen uses the ISMS framework and risk management to demonstrate its compliance.

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes,
- cookies (and similar technologies),
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Where PECR differs from DPA is that it applies to both personal data of a living individual (as in the DPA), and in other business to business data which would traditionally fall outside of DPA scope.

PECR focuses on direct marketing, tracking technologies and the use of them in relation to the privacy rights of individuals, and insists on only holding data with a lawful basis, ensuring consent is gained from data subjects, such as the ability to opt-out of cookies, the use of appropriate privacy notices, and permitting data subjects an opt-out for any material sent to them from us. PECR, requires Citizen to have a legal basis for processing such as consent and allowing customers to opt-out of cookies and provide appropriate privacy notices.

Citizen will put in place controls to limit the risk to the business which, due to the fast-changing nature of security threats include any technological controls which are commercially viable, practicable and effective. However, this does not negate the responsibility of the end users' adherence to the Policy or the Citizen Data Rules or any other guidance notes. A suite of guidance notes is produced to support this Policy, including dealing with Subject Access Requests, data breaches and technical appendices, with detailed technical controls. Colleagues are reminded that ICT is provided for exclusive business use, and all are responsible for complying with policies and procedures in respect of that.

Furthermore, controls will be put in place to ensure that data is shared appropriately and, where data is shared with a third party, we are satisfied they have a robust approach to safeguarding our data.

Failure to adhere to the UK GDPR and Data Protection Act 2018 poses a risk to the business which could result in the alteration, theft, destruction or loss of ability to process Citizen data; some of which is of a confidential or sensitive nature. Should this data become compromised then Citizen could face significant fines for failing to protect it adequately as required by the Act. This could seriously damage Citizen's reputation.

This Policy meets the requirements of the Regulator of Social Housing (RSH) and its revised regulatory framework for England. In regulating the economic standards and in particular the Governance and Financial Viability standards, the RSH requires registered providers to:

- manage their affairs with appropriate skill, independence, diligence, effectiveness, prudence and foresight;
- adhere to all relevant laws;
- and safeguard taxpayers' interests and the reputation of the sector.

As part of this Policy we will consider guidance issued by the Information Commissioners Office (ICO), and our registration responsibilities as advised by the ICO. Where necessary we will amend working practices to reflect new guidance issued.

This Policy recognises that Citizen is required to provide certain information to people under the Social Tenant Access to Information Requirements (STAIRs) under the Social Housing (Regulation) Act 2023. A UK Government consultation process ended in July 2024, at the time of writing, we are awaiting the final version of STAIRs. However, Citizen will respond to requests where either law dictates or where it considers it appropriate to respond due to its openness with customers.

The Data Protection Officer will undertake an Equality Impact Assessment and ensure that any new requirements are identified and incorporated into this Policy where appropriate.

4. Roles and responsibilities

Role	Responsibility
Senior Leadership Team (SLT)	The effective implementation of this Policy; including: *Director of ICT:* Management responsibility for ensuring the high availability of information systems and data, the protection of information systems from loss of integrity (including Disaster Recovery) and the protection of information from inappropriate disclosure. Performs the delegated role of Senior Information Risk Owner (SIRO) from the Chief Finance Officer. The SIRO role requires risk assurances from the Data Owners (Directors). The Information Steering Group (ISG) meeting is chaired by the Chief Financial Officer. The Director of ICT manages Citizen's Data Protection Officer.
Data Protection Officer (DPO)	*Head of Information Governance & Cyber:* Citizen must ensure the DPO is involved, properly and in a timely manner in respect of the processing of personal data. DPO must be provided with appropriate resources and must be able to report to the highest management level. Data Subjects may contact the DPO in respect of their rights under UK GDPR and DPA 2018. Citizen must ensure that the DPO operates independently and will not be instructed in the discharge of their tasks as laid out in law. The DPO must not be instructed to carry out tasks that represent a conflict of interests. The DPO will perform duties, in line with the law, that are informative, advisory and of monitoring compliance

	with the legislation and Citizen Policy. The DPO acts as the official Citizen contact point with the ICO.
All Managers	Have the responsibility and authority to ensure that their staff comply with this policy, ensuring prompt communication when data or systems are compromised. Ensure staff are aware of their responsibility in relation to data and information security, acting with integrity at all times and adhering to the Citizen Data Rules of the organisation. Support the use of appropriate controls for data quality and accuracy.
Data Owners (DOs)	Are members of SLT who provide assurances on risks associated with information assets to the SIRO through the ISG. DOs maintain and manage information assets through assurances from their senior managers. Ensure appropriate controls for data quality and accuracy are deployed. Document any continuity requirements of information systems under their ownership upon request and guidance from Citizen Business Continuity. DO's will make reasonable adjustments to ensure customers are not disadvantaged when receiving or using services because they have a disability or vulnerability.
All Staff	Ensure the security of their workplace and business operation. This includes: • Report any security and data breaches. • Use unique usernames and passwords, and do not share them or write them down. • Wear ID badges in all office locations. • Treat confidential information with appropriate care. • Adhere to the Citizen Data Rules. • Store data appropriately and within the correct systems as required by the Citizen Data Rules. • Take appropriate steps to ensure accuracy and quality of data.

Citizen recognises that data and information security is an important consideration when dealing with sensitive and confidential material as a result of which we will maintain a documented set of rules for end users to ensure best practice is followed.

5. Policy Governance

It is the responsibility of the Board to seek assurance that this Policy is successfully implemented.

The Director of ICT has responsibility for the effective publication, management, training, day to day application of the Policy. The Director of ICT is responsible for signing off this Policy.

Managers are responsible for ensuring that their team have undertaken the appropriate Policy eLearning and training,

Any changes to this Policy must be made in line with the requirements set out in Citizens Standing Orders and our Policy framework.

6. Monitoring and review

The next Policy review is scheduled for 2028 and then every 3 years thereafter. It will be reviewed earlier if there are:

- Any major security breaches
- Any major changes to the nature of technological threats
- Any changes to legislation that materially impacts this Policy

The success of this Policy will be measured by:

- The number of security breaches reported to the Information Commissioner (the target is 0)

Monthly reporting is in place for training and KPI's. Regular updates are provided to the Information Steering Group/ Performance will be reported annually to the Audit and Risk committee.

7. Equality Impact Assessment

This policy reflects Citizen's values, and as such, our staff and others covered by the scope of this Policy are committed to not discriminate against any individual or groups and will respect the diversity of the communities with which we work. We will adhere to our statutory obligations set out in the Equality Act 2010.

In framing this Policy, our staff are committed to not discriminate adversely against any group and will respect the diversity of the communities we are working within.

The Belonging & Inclusion Strategy sets out our commitment to improving the lives of all our customers and making our society a better place for everyone. We want to ensure that all our customers have a meaningful voice, and that we provide them with the best customer experience. In line with our legal and regulatory duties we must ensure that the

services we provide are accessible, and where possible are tailored to the individual needs of our customers.

8. VERSION CONTROL

VERSION	DATE	AMENDMENTS	APPROVED AT/BY	REVIEW
V 1.0	Mar 19	Change of DPO	CO-TERMINOUS BOARD	Jul 2020
V 1.2	Aug 19	Policy in new brand format	CO-TERMINOUS BOARD	Jul 2020
V1.3	August 2021	Review	Board	August 2023
V1.4	February 2022	Updated roles and responsibilities to reflect new Information Steering Group	Board	February 2025
V2.0	February 2025	3-year review – Contractors added into the scope of the Policy and key obligations for all staff, contractors and suppliers. Setting out the ISMS principles for managing data, procedural safeguards and employee expectations. Format changes into new template Addition of DPO into Roles and Responsibilities.	Board	February 2027