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 (GDPR) and, the Data Protection Act 2018 which became law on 25th May 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 Data Protection Act 2018
- Ensure compliance with the Privacy and Electronic Communications Regulations (PECR)
- Protect Citizen's Information Assets
- 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.

2. Purpose

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

3. 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 devised used on Citizen premises or connected to Citizen resources that are capable of processing or storing Citizen's information.

4. Roles, responsibility and authority

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.
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 (DA's)	Provide assurances on risks associated with information assets to the SIRO through the ISG. DA's 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.
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.

5. Policy management and system requirements

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 provide a documented set of rules for end users to ensure best practice is followed. This is supplied within the attached appendices.

Citizen employees will act in line with the requirements of GDPR and the Data Protection Act 2018 and its six 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 are 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 GDPR in order to safeguard the rights and freedoms of individuals; and

- 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."

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 also 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.

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 data rules or any other guidance notes. A suite of guidance notes are 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 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 law
- and safeguard taxpayers' interests and the reputation of the sector.

This policy will take into account guidance issued by the Information Commissioners Office (ICO), and our registration responsibilities as advised to the ICO. Where necessary we will amend working practices to reflect new guidance issued.

This policy recognises that Public Authorities are required to provide certain information to people under the Freedom of Information Act 2000. At the time of writing this policy Citizen is not yet deemed to be a public authority for all of its activities and are therefore not required to provide information under the FOI Act. However, Citizen will respond to requests where either law dictates or where they consider it appropriate to respond due to its openness with customers.

6. The Data Protection Officer (DPO)

Citizen is committed to ensuring that legal compliance and best practice in respect of data protection are appropriately embedded across all of its operations and is routinely considered in all of its business activities, policies and processes. This work will be championed by Citizen's Data Protection Officer. (DPO)

Citizen has assessed its requirements under GDPR and has concluded that its processing activities are such that it meets the requirements for a mandatory data protection officer.

The DPO's minimum tasks are defined in Article 39 and will be as follows:

- To inform and advise Citizen and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

The DPO will have an appropriate level of experience and professional training to competently carry out the duties of the role and will report directly to the Board and will act with independence in data protection matters in this role. All Board Members however will have access to the DPO.

The Data Protection Officer for Citizen is Shane Murphy.

7. Implementation, monitoring and review

The next policy review is scheduled for 2023 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 technology 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. Performance will be reported annually to the Audit and Risk committee.

8. Supporting documentation and procedures

Please see the following policies and procedures:

- Code of Conduct policy
- ICT Acceptable Use Policy
- Subject Access Standard Operating Procedure
- Data Privacy Impact Assessments (DPIA) – Process and Results Template
- ICT AUP DP Standards
- Data Rules