Governance and Financial Viability Policy

6

DATA PROTECTION

This document forms section six of Victory Housing Trust's Governance and Financial Viability Policy

Last Reviewed July 2018

If you would like this policy in Large, Print, Audio, Braille another language or an alternative format please contact our customer services team on 0330 123 1860 and we will do our best to help

6. Data Protection Policy

6.1 Introduction

Victory Housing Trust (Victory) is fully committed to compliance with data protection law including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("the Act"). Victory will therefore follow procedures that aim to ensure that all employees (including temporary and agency workers), Board and Committee members, involved residents contractors, agents, consultants, partners or other persons involved in the work of Victory and who have access to any personal data held by or on behalf of Victory are fully aware of and abide by their duties and responsibilities under the Act. The Act provides that most processing of personal information is subject to the GDPR.

6.2 Policy Statement

6.2.1. In order to operate efficiently, Victory has to collect and use information about people with whom we work in order to carry out our business and provide our services. These may include our tenants, and former tenants, other customers, members of the public, current, past and prospective employees, Board and Committee members, and suppliers. In addition, Victory may be required by law to collect and use certain types of information. This personal information must be handled and dealt with properly, irrespective of how it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this is undertaken.

6.2.2 We will appoint a Data Protection Officer to manage day to day activities and training. Compliance will be reported to the Leadership Team and Audit Committee. Where appropriate we will seek external legal Data Protection expertise to support Victory in all data management and protection matters.

6.2.3 The Leadership Team are responsible for ensuring maintenance of Victory's data asset register which sets out among other things where the data is stored, why it is collected and how it is protected.

6.2.4 We will not attempt to gain access to information that is not necessary to hold, know or process. All information that is held will be relevant and accurate for the purpose for which it is required and will be kept secure at all times. It will be deleted or anonymised (made non-personally identifiable) as soon as possible in the life cycle.

6.3 Purpose

6.3.1 The purpose of this policy is to ensure any personal data we collect, record or use in any way whether it is held on paper, computer or other media will have safeguards to ensure that we comply with the Act.

6.4 Principles of Data Protection

6.4.1 Victory, adopts the seven key principles of GDPR both as a basis for ensuring compliance with the Act, and also for ensuring the privacy and confidentiality of individuals. These are summarised below:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

6.5 Data Definitions

6.5.1 The Act is designed to protect the individual and their personal data, which is held and processed on their behalf.

- **Data:** Any information which can be held manually or on electronically.

- **Data Controller**: The body which determines the purposes and manner in which personal data is processed – this means Victory Housing Trust is a Data Controller.

- **Data Processor:** A body which may process person data on behalf of Victory, for example a Local Authority Housing Benefit Office or a maintenance contractor, etc.

- **Data Protection Officer:** The person who monitors internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the Information Commissioners Office. This role is supported by the Deputy Chief Executive and will have a direct reporting line through to a non-executive director. At present this is the Chair of the Audit Committee.

- **Data processing**: Any action involving personal data, including organisation, disclosure, deletion, obtaining, recording, retrieval, and consultation.

- **Data Subject:** Any living individual who is the subject of personal data, whether in a personal or business capacity.

- **Personal data:** Any information from which a data subject (natural living person) is identifiably or can be identified, such as:
    - Name, address, phone number, National Insurance Number, Date of Birth.
    - Household composition, marital status.
    - Financial circumstances, income, rent account details.
    - Online identifiers such as IP address

- **Special categories of personal data**: Personal data, the disclosure of which may pose a greater threat to individuals, such as:
    - Racial and or ethnic origin
    - Religious or similar beliefs
    - Mental or physical health
    - Proceedings for any offences committed/alleged
    - Political opinions
    - Membership of a trade union
    - Sexual life
    - Biometric and genetic data

6.6 Disclosure / Processing of Information

6.6.1 Victory considers all personal information given by its employees and customers as confidential, and any unauthorised disclosure of any such information is treated very seriously. However, in the following situations we need not request prior consent:

- As part of a fraud investigation;
- In order to comply with the law;
- In connection with legal proceedings;
- Where it would be essential for Victory to carry out or fulfil our regulatory or statutory duties; and
- Anonymously for statistical or research purposes

6.6.2 Victory has Information Sharing Protocols with a number of partner organisations. This allows us to share specific data between agencies for the benefit of individuals and the community. This information is not shared with organisations where there is no protocol. All information sharing protocols Victory engage in will be authorised by the appointed Director and Data Protection Officer to ensure compliance with our controls and the Information Commissioner Code of practice for information sharing.

6.6.3 We will not transfer personal data to jurisdictions outside the European Economic Area (EEA) unless that country has a recognised adequate level of protection for data protection purposes. We may process and publish information outside the UK as part of our World Wide Web activities (internet). This information may at times relate to individuals personal data. When this is the case we will ensure the individuals have given their informed consent to this type of processing.

6.6.4 We will ensure Data Processing obligations are applied to all contracts and management agreements where we are the ‘Data Controller’ contracting out services / processing of personal information to another party known as a ‘Data Processor’. These will outline roles and responsibilities.

6.6.5 We will comply with our policies and practices when exploring or entering into any acquisition or merger. We will ensure all personal or sensitive personal information is anonymised as part of any evaluation of assets and liability assessments except as required by law.

6.6.6 We will ensure privacy statements are in place and made available to all our current and former residents, applicants, leaseholders and freeholders advising our approach and obligations in respect of Data Protection Victory will follow.

6.6.7 We will operate a document retention procedure which establishes how long it is appropriate to hold documents and information. Documents and data that are no longer required will be destroyed in a secure manner and in some circumstances be returned to you.

6.6.8 We will maintain appropriate cyber security controls and set these out in our cyber security procedure document. This will cover the protection of networks, mobile devices, data, and staff training.

6.6.9 We will operate CCTV cameras to record images and audio for the purposes of maintaining safety for staff and visitors, training, detection or prevention of crime and security. CCTV audio and images will be kept securely at all times and will be kept for a long as they are required and then destroyed. Appropriate signage will be displayed in all areas covered by CCTV. Access to the data will be limited to those operating the system and requests for information will require senior manager approval and will be logged.

6.6.10 We will record telephone calls for training and monitoring purposes. Recordings will be kept securely at all times and access to them restricted. The recordings will be retained for as long as they are required and then destroyed.

6.7 Individual Data Subjects: Information Access

6.7.1 We recognise individuals have the right to make a request for a copy of their personal information held about them on computer and in relevant manual paper based filing systems. We will respond to the data subject or their representative within one calendar month of the request being deemed valid. A valid request will be when the following conditions have been satisfied.

- We will process requests once we are satisfied of the identity of the data subject
- We have sufficient information to enable the request to be processed;
- Proof of authority when data subjects engage a representative to act on their behalf.

6.7.2 We recognise the rights of individuals to prevent processing causing damage or distress to them, in relation to automated decision making and to prevent processing for direct marketing purposes.

6.8 Breaches of the Data Protection Policy

6.8.1 Breaches of data protection will be thoroughly investigated and where appropriate and proportionate reported to the Information Commissioner and affected individuals. Incidents will be reported to the Audit Committee.

6.8.2 We recognise and understand the consequences of failing to comply with the requirements of the Data Protection Act 2018 may result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- The Information Commissioner, (ICO) suspending or withdrawing the right to process data;
- Loss of confidence in the integrity of our systems and procedures;
- Damage to reputation.

6.8.3 We may consider taking internal disciplinary or legal action where employees, Board and Committee members, involved residents, contractors, agents, consultants or partners do not comply with the Data Protection Act 2018 and our governance controls (strategies, policies, procedures and training) in relation to this matter. Any such person will not disclose personal information to other parties without first seeking consent from Victory and/or if they are required to do so by law and/or where non-disclosure would result in that person being guilty of a criminal offence.

6.9 Complaints

6.9.1 Complaints relating to alleged breaches of the Act and/or complaints that individual's personal information are not being processed in line with the seven key principles will be managed and processed by the Data Protection Officer and the Deputy Chief Executive. Concerns can also be reported directly to the Information Commissioner who will consider if Victory has broken any of the data protection principals and establish whether or not we are processing information in accordance with the Act.

6.9.2 We acknowledge that the court will grant compensation to a data subject if it is found the data controller has contravened the requirements of the Act and as a direct consequence a Data Subject has suffered damage and distress. We recognise that we are also responsible for the actions of Data Processors.

6.10 Roles and Responsibilities

6.10.1 The Board has overall responsibility for this policy.

6.10.2 The Chief Executive is responsible for overseeing the implementation of the policy.

6.10.3 Directors and Managers are responsible for ensuring that all aspects of their services comply with the policy.

6.10.4 Employees are required to ensure that they act in accordance with the policy in carrying out their duties. We will ensure all employees are fully trained and promote the awareness of good data management, security and protection

6.10.5 All contractors who are users of personal information supplied by Victory will be required to confirm that they will abide by the requirements of the Act and this policy with regard to information supplied by Victory.

6.11 Implementation and Monitoring

6.11.1 We are committed to ensuring that all our governance controls are proportionate and appropriate. We will monitor the effectiveness of this policy and recommend policy changes to improve service delivery. To this aim we will carry out an annual review taking account of legislative and regulatory changes and a fundamental review of this policy every three years.

6.11.2 We will operate as part of our information governance controls a set of registers which will be kept securely and reported to the relevant committee, Leadership Team and Board:

- Breach Register
- Subject Access Requests
- Requests under the individuals rights
- Data Processors
- Information Sharing Protocol

6.12 Legal References

6.12.1 The key primary legislation and guidance underpinning this policy is as follows:

- Data Protection Act 2018
- Human Rights Act 1998
- General Data Protection Regulations (GDPR)
- Protection of Freedoms Act 2012 (Part 2 Regulation of surveillance)
- Freedom of Information Act 2000 (Whilst not governed by this act, we will consider and reply appropriately and proportionally to requests for business information)