Victory Housing Trust - Data Sharing Protocol

Victory shares appropriate resident and property data with its contractors and partners to enable them to deliver effective services. Victory requires contractors and partners to provide performance and delivery data to Victory, to enable service monitoring and to maintain a full Victory record of services delivered for Victory residents and properties.

This protocol describes in broad terms the data that Victory expects to share and receive; the nature of the ICT infrastructure required; the level of compliance required; to manage the secure transfer and processing of Victory data.

1. Resident & Property Data

1.1. Victory will share appropriate data, including Personal Data as defined by the Data Protection Act 1998, with contractors and partners. Such data will be adjusted to meet the specific needs of the contract/service but will typically include:

- Property data (property address, property type, build type, components, etc)
- Resident data (names, ages, gender, vulnerabilities, etc)
- Operational data (Victory staff contacts, processes, procedures)
- Security & safety data (visit in pairs, dangerous dogs, presence of asbestos, etc)

1.2. Data may be provided through controlled access to Victory systems or through exports of data to contractor/partner systems. Regardless of the method, Victory requires contractors and partners to hold and to process such data securely and appropriately, and for personal data to be processed in such a way as to comply entirely with the requirements of the Data Protection Act 1998.

2. Performance and Delivery Data

2.1. Victory will usually require contractors and partners to use Victory systems to record performance and delivery data, such data will depend on the nature of the contract/service but will typically include:

- Details of contacts and transactions with Victory residents.
- Details of works (e.g. repairs & maintenance) carried out to Victory properties.

2.2. Where relevant data cannot be directly recorded in Victory systems Victory will require an agreed dataset to be transferred to an agreed format and schedule (daily, weekly or monthly depending on the data), either via file export or through an interface depending on circumstances.

3. ICT infrastructure and support

3.1. Victory requires its contractors and partners to be able to receive, store and process all shared data within an Information Technology infrastructure that has been professionally installed and is professionally supported, specifically:

3.2. Victory data must be held securely behind robust password protected accounts and devices, and protected by robust and current firewall and anti-virus regimes.

3.3 The contractor/partner IT infrastructure must include a reliable internet connection of sufficient capacity to enable connection and interfacing with Victory systems

3.4. Victory data will be exported in electronic format in the current versions of Microsoft Excel or Word. Contractors/partners must have the facilities to be able to store and process such formats, and where required export such formats via a secure FTP site hosted by the contractor/partner.

3.5 Victory expects contractor and partner systems to be TLS 1.2 compliant, specifically support for TLS 1.0 or earlier (SSL V3) encryption protocols should be disabled.

4. Contractual and compliance

4.1. Victory's data sharing protocol is a standard component of the Statement of Requirements within our procurement process.

4.2. The storage and accessing of Victory data must be evidenced by the contractor/partner as compliant with the requirements of Victory's internal audit requirements for data security. Victory may extend its internal data security audit process to include contractors/partners.

4.3. When the contract/service ends Victory will require the contractor/partner to:

- Destroy all personal data supplied by Victory, and confirm in writing.
- Provide Victory with any outstanding performance and delivery data.

****