Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

If you have any queries about your rights in relation to how we collect and store your personal information please speak to your manager or HR

10.4 – IT DATA SECURITY POLICY

Purpose and Scope

This policy provides details about Data Security (see Annex for Definitions of capitalised terms) and technical details about secure storage and transmission of data by the IT Department at Elizabeth Finn Homes Limited.

Some IT facilities are operated for Turn2us (of which Elizabeth Finn Homes Limited ('EFHL') is a wholly owned subsidiary) and consequently this policy applies equally to any such IT resources.

The scope of the data security section of this document is all data stored in the EFHL and for Turn2us in EFHL on-premise IT systems.

Data Security

The IT Department takes measures to store and manage the data it is responsible for both securely and effectively, to avoid detriment to the organisation and its data subjects. These measures are typically a compromise of security, encryption, recoverability (in the event of an IT disaster) and cost.

Where the IT department is not directly responsible for the data storage (for example when an off-site hosted provider ('in the cloud') is used, the IT Department must be consulted to ensure that the data transport, storage and security being offered by the third party meet the security and technical requirements.

The data security measures taken by the IT department are summarised as follows:

Data on PCs and mobile computing devices	Users are required by the IT Use policy not to store Personal Data or business sensitive data locally on PCs or mobile computing devices. Instead they are required to use the organisations remote computing platform. Where this is not technically possible (e.g. data on mobile phones and similar devices) device encryption must be employed together with a suitable PIN/password. The ability to 'remote wipe' devices is employed where possible.
Organisational data stored on the IT Departments server platforms.	The server platforms operate a RAID system to store data in a way that protects against failure of a disc, but also means that no recoverable data resides on a single disc, or is readable outside the system on which is was implemented.
Disc, file and database encryption	Discs, files and databases are not currently encrypted in the organisation. This is for reasons of cost, performance and recoverability in the event of a disaster. At present it is thought the advantages are outweighed by the risks and costs involved.

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

If you have any queries about your rights in relation to how we collect and store your personal information please speak to your manager or HR

10.4 – IT DATA SECURITY POLICY

	Where possible, laptops are encrypted. There is a decreasing number of older devices where this is not possible, The risk is mitigated by staff being required to use remote computing and not store Personal or business data locally.
Transport of data encryption	Network transports within the organisation are all encrypted using IPSec VPNs. The typical level of encryption is AES-128. SSL VPN is provided for remote users typically using an encryption level of TLS >=168 bit.
Email encryption	Opportunistic TLS encryption for all email with enforced TLS for key data processing partners
Pseudonymisation	Pseudonymisation is not applicable to the data held by the IT Department about its users. For Turn2us data, pseudonymisation is explained within their data policies.
Internal penetration testing	IT Department penetration testing is done internally as part of any network change. Externally facing web-tools such as e-mail and multi-factor authentication interfaces are tested using industry standard online testing kits such as Qualsys SSL Labs and Gibson Research Shields Up. Certain services (such as e-mail) are run at a level of service which offers what the IT Department considers an acceptable compromise of adequate security vs compatibility/usability vs cost. This is reviewed annually, as part of policy review.
External penetration testing	External penetration testing is conducted on most public IP addresses used by EFHL.
Removable media drives	Where possible these are disabled on thin clients. However, in certain circumstances USB and media drives may be opened for business purposes. The IT use policy discusses their safe use.

Assessment Tools

The IT Department uses the NHS Data Protection Toolkit as its main self-assessment tool. Although not ideal, we are required to comply with it to interface with NHS systems.

Protective testing is undertaken after major system and network changes using industry standard tools such as those from Qualsys and Gibson Research, and then changes and retest made accordingly. External penetration testing of public IP addresses is undertaken on an ongoing basis by a third party for all IP addresses used to provide on-premise services and also a single care-home (the other care homes are duplicates).

Copies of all EFHL HR Policies can be found on the Intranet. All EFHL Staff are subject to EFHL HR Policies. EFHL HR Policies are non-contractual, are reviewed regularly and may be subject to change. All queries on the application or interpretation of this policy should be raised with the Head of Department or HR.

If you have any queries about your rights in relation to how we collect and store your personal information please speak to your manager or HR

10.4 – IT DATA SECURITY POLICY

Annex 1 - Definitions

Data Retention	The continued storage of an organisation's data for compliance or business reasons.
Data Security	Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption.
Leaver/Leavers	A User who has stopped using or accessing the IT systems.
Personal Data	Personal Data means data which relate to a living individual who can be identified – (a) from that data, or (b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
RAID	Redundant Array of Inexpensive Discs. A mechanism to spread data across multiple data disc drives in such a way that no one disc has recoverable data, but also that a disc can fail and the data be rebuilt from information on the other discs in the array.
Sensitive Personal Data	A DPA definition that means data about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, criminal record, criminal proceedings relating to a Data Subject's offences
Special Categories of Personal Data	A Data Protection Act 2018 (UK GDPR) category of data which is more sensitive that othe Personal Data and specifically includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics for ID, health, sex life and orientation. It does not include data relating to criminal offenses and convictions, because these are addressed by specific safeguards elsewhere in the Act.
User/Users	A collective term used for Turn2us and EFHL trustees, employees, contractors and agents including voluntary agents who use or access the IT systems.

//End