

ELIZABETH FINN HOMES LIMITED

exceptional care for the individual

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

10.3 - IT DATA RETENTION POLICY

Purpose and Scope

This policy provides details about Data Retention for Personal Data (see Annex for Definitions of capitalised terms) held by the IT Department at Elizabeth Finn Homes Limited.

The scope of the Data Retention section of this document is Personal Data held by the IT department to be able offer its services (it does not hold any Special Categories of Personal Data). This is typically User identification, contact and password information.

Some IT facilities are operated for EFHL's parent organisation, Turn2Us. This document does not define data retention for the information that EFHL or Turn2us departments and Users store on the EFHL IT systems.

Personal Data held by the IT Department

The IT department keeps a minimum of User's Personal Data to be able to deliver the IT provision. This includes, but is not limited to:

- name'
- personal telephone numbers (typically for multi factor authentication);
- personal email addresses on occasion (typically for contact and multi factor authentication);
- personal security question answers (for password reset, multifactor authentication etc.);
- IP addresses and meta data for people connecting to our services (to allow systems to work and mobile devices to be managed);
- Contents of emails plus personal and departmental drives.

Note that passwords are always stored in an encrypted form.

Data Retention

The following is the IT Department policy for the retention of data:

System that hold Personal Data	Retention Period	Comments
Active Directory account information	Up to one year after leaving	Accounts are disabled when Users leave the organisation. However, because some Users return, we often keep account disabled and segregated into a separate organisational unit with Active Directory to allow restoration if required. Account information is typically purged twice annually.

ELIZABETH FINN HOMES LIMITED

exceptional care for the individual

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

10.3 - IT DATA RETENTION POLICY

		Also see notes below on backup data sets.
Email accounts on system	Up to one year after leaving	Managed as part of the Active Directory management process. Email account contents of Users who have left are then exported to offline storage.
Archived offline email and user account content	Up to seven years after leaving (for finance staff) but typically three years	This is for business continuity. Experience shows that some Users who have left have inadvertently stored business critical information in emails or User folders. Storing securely offline mitigates the business risk whilst reducing danger of Personal Data breach.
Virus scanning and store and forward of email from cloud security provider	Quarantines and 'store and forward' are automatically deleted after forwarding or, depending on User activity, up to 30 days later.	Information and quarantines are held in EU datacentres by reputable providers.
Multi-factor authentication Personal Data for SSL VPN remote access (and web-mail from late-2018)	Up to one year after leaving – as per Active Directory	Purge of MFA accounts for Users who have left as part of twice annual account data purge.
Management of back-up data sets for files and databases	Up to 4 months of data is held in online and offline data backups of user and departmental files and databases. This is likely to contain Personal Data stored under the retention policy of each department.	The deletion process is automatic apart from manual backups which are reviewed annually.

Technical Guidance of Application of Data Retention Policy

The following is a technical summary of the process that ensures that the data retention policy is met.

ELIZABETH FINN HOMES LIMITED

exceptional care for the individual

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

10.3 - IT DATA RETENTION POLICY

1. Twice yearly purge of Active Directory and related data. This is typically performed in June and December each year.
 - a. A list is printed of all User names in the Active Directory and shared with HR to identify Leavers (this ensures that leavers where IT have not been informed are identified) along with a flag for those who have been going 6 months or more. This Leavers list is the basis for the next steps.
 - b. In the email system, mailboxes for leavers over 6 months are exported to standalone email archive files (.pst) which are then stored on DVD or USB memory and securely stored in the IT safe.
 - c. Content from Leavers' file server 'users\$' and 'home\$' directories is also backed up to offline storage and stored in the same way as (b). Profile\$ and user profile discs are just deleted (as they shouldn't hold Personal Data or business critical data).
 - d. Offline storage older than three years for (b) and (c) are erased, except for key finance staff, where it may be held seven.
 - e. The user list on the multifactor management server is checked and anyone on the Leavers list is deleted, including those leavers less than six months. Accounts can be recreated if there is a returning User.
 - f. Those Leavers who have left more than six months ago are deleted from Active Directory. Manual checks are made to ensure recent Leavers (6 months or less) are 'disabled' and stored in the Leavers organisational unit (OU).
 - g. A check is made to ensure manual financial database backups older than 7 years are deleted.

Automatic backups are monitored automatically as part of system monitoring.

ELIZABETH FINN HOMES LIMITED

exceptional care for the individual

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

10.3 - IT DATA RETENTION POLICY

Annex 1 - Definitions

Data Retention	The continued storage of an organisation's data for compliance or business reasons.
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.
Sensitive Personal Data	A DPA 1998 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 than other 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.
SSL VPN	A method of Virtual Private Network using a secure web browsing system that allows remote users to securely connect to our servers.
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.