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

10.0 - I.T. ACCEPTABLE USAGE POLICY

Purpose and Scope

This Acceptable Usage Policy covers the security and use of all of Elizabeth Finn Homes Limited (EFHL) information systems and information technology ('IT') equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all of EFHL trustees, employees, contractors and volunteers.

This policy applies to all information, in whatever form, relating to EFHL business and to all information handled by EFHL relating to other entities with whom it deals. It also covers all IT and information communications facilities operated by EFHL or on its behalf.

Some IT facilities are operated for EFHL's parent organisation, Turn2Us. Consequently, this policy applies equally to any individuals using these resources.

Computer Access Control – Individuals Responsibility

Access to EFHL IT systems is controlled by the use of User IDs, passwords and/or tokens (such as a one-use PIN code or mobile phone authentication). All User IDs and passwords/tokens are uniquely assigned to Individuals and consequently Individuals are accountable for all their actions on EFHL IT systems.

Some shared resources are accessed by a 'Workstation ID' and password with access to individual information systems therein being controlled via uniquely assigned User IDs and passwords, for which Individuals are accountable for their actions. An example of this is the shared care station terminals in EFHL, which have a shared Workstation ID and password, and Team Member User IDs and passwords for the applications within, where Individuals are responsible for their actions (e.g. logins to databases such as eRoster or iCare).

Individuals must not:

- Allow anyone else to use their user ID and password/token on any system.
- Share any Workstation ID and password with anyone not authorised to use the device.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected (for example by writing it down) or circumvent password complexity or renewal requirements.
- Perform any unauthorised changes to EFHL IT systems, networks or information.
- Attempt to access data that they are not currently authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-EFHL authorised device to the network or IT systems (with the exception of the guest Wi-Fi network).
- Store EFHL data on any non-authorised equipment.
- Give or transfer EFHL data or software to any person or organisation outside EFHL without the authority of their manager.

Line managers must ensure that Individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

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

10.0 - I.T. ACCEPTABLE USAGE POLICY

Internet and Email Conditions of Use

EFHL Internet access and email is intended for business use. Personal use of Internet access is permitted with agreement from the Line Manager where such use does not affect the individual's performance, is not detrimental to EFHL in any way, is not in breach of any term and condition of employment and does not place Individuals or EFHL in breach of statutory or legal obligations. Personal use of EFHL email is strongly discouraged, although it is recognised that it is not always possible to entirely separate personal email from legitimate business use. EFHL are not responsible for the security or privacy of personal material that is stored or transmitted using EFHL information systems.

All Individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which EFHL considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email system(s) in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to EFHL, alter any information about EFHL or express any opinion about EFHL, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward EFHL email to personal email accounts (for example a personal Gmail or Hotmail account) without explicit written consent from the IT Director or authorised deputy.
- Make official commitments through the internet or email on behalf of EFHL unless authorised to do so. If in doubt the individual's line manager should be consulted.
- Download copyrighted material (for example image, music, film or video files) without appropriate approval.
- Infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect EFHL devices to the internet using non-standard connections or connections not approved by the IT department.

Wi-Fi

Most EFHL sites offer a Wi-Fi service for resident / visitor use. Individuals use is subject to the Wi-Fi Terms & Conditions document that is currently in place. With the exception of

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

10.0 - I.T. ACCEPTABLE USAGE POLICY

EFHL mobile devices (including mobile point of care devices), the Wi-Fi service is not intended for conducting EFHL business unless previously agreed with the IT department.

Clear Desk and Clear Screen Responsibility

In order to reduce the risk of unauthorised access or loss of information, Individuals must adopt a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using any security features provided (e.g. secure electronic document storage, locking cabinets for paper).
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password/token when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- Confidential printed matter must be shredded / disposed of in confidential waste bins.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with the appropriate EFHL flexible or remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Personal data or sensitive business information must not be stored on laptop computers, but instead the VPN facilities used to remotely work on the servers. Unsecured public Wi-Fi (public hotspots or open networks) must not be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and similar devices. They must be protected by at least a password or a PIN and encryption.

Telephony (Voice) Equipment

With regard to both voice (landline) and mobile phone equipment, Individuals must not:

- Use EFHL voice equipment for conducting private business (other than in accordance with the mobile phone provisions below).
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or international operators.
- Access premium rate services without line manager approval. Note that facilities such as conference call recording often attract premium rates.

Voice (Landline)

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

10.0 - I.T. ACCEPTABLE USAGE POLICY

Use of EFHL' voice (i.e. 'landline' or 'cordless') equipment is intended for EFHL business use. Use must comply with this and other appropriate EFHL policies. Individuals must not use the voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at Individuals own expense using alternative means of communications.

Mobile Telephones, Smartphones and Similar Devices
Individuals may be issued with an EFHL mobile telephone/smartphone (mobile device) for use as part of their work. Individuals using an EFHL mobile device are subject to the following terms:

- Use must comply with this and other appropriate EFHL policies.
- Use must comply with equipment manufacturer and mobile carrier terms and conditions.
- Loss of a device must be reported immediately to the IT department and the network operator.
- Individuals are required to take good care of any device allocated to them. Normal wear and tear is to be expected, but any damage to a device or accessories must be reported to the IT department who will advise on and authorise any repair. In the event of carelessness, loss or damage EFHL reserves the right to withdraw the device, issue an older or lesser model or change the provision entirely (for example, by providing an allowance toward a personal device).
- The mobile device must be immediately returned to EFHL on demand from the Director of IT, an authorised deputy or the HR department.
- EFHL permits the use of the mobile devices for reasonable personal voice and data purposes, providing that any voice and data allowances are managed so that the individual's work can be conducted without incurring additional expense. The call and data allowances associated with devices will be advised from time to time.
- Data on mobile devices for work and legal retention purposes is the property of EFHL. This includes, but is not limited to, email, calendar and contact information.
- Applications and personal data added to the mobile device by the user will be returned to the user only as far as is practicable after the phone is returned to the organisation. This does not prejudice in any way existing HR guidelines and procedures, which may take precedence.
- EFHL reserves the right to analyse mobile telecoms bills to observe the pattern of usage and if appropriate ask any individual for reimbursement of the cost of excessive non-business use or inappropriate business use.
- Voice and data roaming (i.e. international use) must be turned off unless otherwise agreed with the IT department. EFHL retains the option to charge Individuals for roaming (overseas) voice and data that is not previously agreed.
- Apart from analysis of mobile bill data, EFHL will as far as possible respect Individuals' privacy related to the content of mobile device personal voice and data, except where law enforcement agencies or similar require disclosure.

Portable Data Storage Devices and Cloud Based Data Storage

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

10.0 - I.T. ACCEPTABLE USAGE POLICY

EFHL do not permit the use of non-approved portable data storage devices such as USB memory sticks, CDs, DVDs and removable hard drives without written approval of the Director or authorised deputy. It is likely that only devices with encryption enabled will be approved, and then only for a limited time period (for example when there is no network connectivity).

Cloud based storage (such as Dropbox) is similarly not permitted without explicit written authorisation from the IT Director or authorised deputy. Instead, Individuals should use the secure remote working methods provided, such as remote VPN and e-mail, or consult the IT department to arrange secure large file transfers to those outside the organisation.

Using Own Equipment

This is commonly referred to as BYOD - Bring Your Own Device.

In general, EFHL do not permit individuals to use their own equipment for work purposes. In no circumstances are individuals allowed to store work data on their own devices, other than the limited email data mentioned below.

In limited circumstances (such as during the Covid-19 pandemic, and where it is agreed that Individuals can used their own smartphone for work), permission may be given to Individuals to use their own equipment. Any such use must be agreed with both the IT department and relevant care home General Manager on a per-device basis. In these circumstances, the following applies:

1. When using a computer: Data must be accessed by either (i) the EFHL remote-working provision (VPN, two factor authentication, remote desktop) with no data stored on the individual's equipment or (ii) web-mail where provided, with any cached data deleted (private mode browsing is recommended) and using any additional security measures provided.

2. When using a phone or tablet for email and calendar access: Instructions will be provided by the IT department on how to do this, and the guidance must be followed. The device must be encrypted. The email system requires the device to have a PIN/password/biometric ID enabled, and this must not be circumvented. The device must be set not to hold more than one month of email data.

3. If the is any concern that a device is lost or compromised then the IT department must be informed as soon as possibe so the appropriate security measures can be implemented. These may require the user to comply with requests to limit/mitigate any potential EFHL data loss.

Software

Individuals must only use software that is authorised by the IT department when using EFHL IT systems and equipment. This includes hosted and other 'cloud' IT arrangements and document files that could contain macros and malware (such as Excel or Word files). Authorised software must be used in accordance with the software supplier's licensing

agreements. All software on EFHL systems and equipment (including hosted and other 'cloud' IT arrangements) must be approved and installed by, or under the guidance of, the EFHL IT department.

Individuals must not store personal files such as music, video, photographs or games on EFHL IT equipment with the exception of, and in accordance with, the provisions made for mobile devices stated above.

Viruses and Malware

The IT department uses various automated virus and malware prevention, detection and management methods. All PCs and thin client terminals have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved EFHL anti-virus software and procedures.

Individuals must immediately report to the IT department any virus alerts or if they suspect virus software is missing, not updating or otherwise disabled or not functioning correctly. If a virus or other malware is suspected, the offending equipment must be turned off immediately and the IT department immediately informed.

Individuals must not knowingly, and take precautions not to carelessly, introduce viruses or other malware into EFHL systems by downloading software or data from untrusted sources (also see 'software' above). Individuals need to be aware of, and guard against, 'phishing' attacks (these are usually e-mails or other communications which attempt to trick the user into giving away information such as passwords) and other emails or communications that trick users into downloading malware (often ransomware) either as an attachment or via an internet link. If in doubt of the origin of an email or other communication, it should not be opened and instead deleted. If an individual thinks they have been 'tricked', then they must immediately contact the IT department via IThelp@efhl.co.uk or via their manager. Emails, phone calls and other media communications can be very convincing, and the IT department like to be aware and help.

Actions upon Termination of Contract

All EFHL equipment and data (for example laptops, mobile devices and charging equipment) must be returned to EFHL at termination of contract.

All EFHL data or intellectual property developed or gained during the period of employment remains the property of EFHL and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data created and stored on EFHL information systems and equipment is the property of EFHL. There is no provision for individual data privacy on EFHL systems, with the limited

exception relating to mobile device data stated above. However, if access to a Team Member's email or documents is required it will be managed by the IT and/or HR departments.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. EFHL has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Web browsing may be content filtered to help protect Individuals.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the Data Protection Act 2018 (UK General Data Protection Regulation (GDPR)), the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with the Computer Misuse Act 1990, the Data Protection Act 2018 (UK GDPR) and the EFHL Data Protection and Confidentiality policy.

Data Protection and Confidentiality, Data Security and Security Breaches

EFHL has a duty of care to its clients (especially those about which it holds Personal Data or Sensitive Personal Data; i.e. its Data Subjects), and considers secure information management a crucial component of its business functions. As part of that Individuals are required to comply with the relevant Data Protection and Confidentiality Policy. As part of that policy, it is each Team Member's responsibility to immediately report suspected, or the potential for, breaches of data or information security without delay.

All suspected breaches of data security will be investigated. The immediate focus will be on containment and mitigation, but where investigations reveal misconduct, disciplinary action may follow in line with EFHL disciplinary procedures.

IT Support / Helpdesk

The IT department offers support via the virtual IT Helpdesk (ithelp@EFHL.org.uk or http://ithelp.finn.org.uk/ at the time of writing). To ensure requests are recorded and dealt with fairly, the IT Helpdesk is the only way support requests are managed. If a Team Member cannot send email, then they should ask their Line Manager or a colleague to report, or as a last resort ring HQ and inform reception who will pass on messages. Individuals should not email individual IT staff with requests for support.

Violation of Policy

Individuals, when requested, are required to co-operate with IT staff in any investigations of IT systems abuse. Refusals to respond to reasonable requests, or attempts to impede investigations, are considered a violation of policy and may result in the suspension of access privileges and disciplinary action.

Any individual's violation of this policy may result in:

- Full investigation of the individual's and others' data files and system resources.

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

10.0 - I.T. ACCEPTABLE USAGE POLICY

- Temporary or permanent restriction or suspension of IT access privileges.
- Disciplinary action.
- Legal action.

Any such action would be taken in full consultation with the HR department.

If you have any query about the content of this policy please speak to your Head of Department or HR.

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

10.0 - I.T. ACCEPTABLE USAGE POLICY

IT POLICY AGREEMENT

In consideration of my being authorised to use EFHL IT facilities, I agree that, unless otherwise instructed by the Director IT, I will adhere to the terms of the IT Acceptable Usage Policy. Furthermore, I understand that serious violation of the policy may result in disciplinary and/or legal action being taken again me.

User's signature: _____

Print User's name: _____

Date: _____

Detach and return to the HR Department.