

Elizabeth Finn Homes Limited

Cloud Applications and IT Use Policy

Owner:	Head of IT
Approved by:	Executive Leadership Team (ELT)
Effective from:	October 2026
Review date:	October 2027
Version:	1.0

This document remains the property of Elizabeth Finn Homes Limited. Release to regulatory authorities is permitted as required. Release to other organisations or individuals may only be authorised by Company Directors.

Table of Contents

1	Purpose.....	2
2	Scope	2
3	Definitions.....	2
4	Cloud System Access & Identity Security	3
5	Acceptable Use of Cloud Applications.....	4
6	Prohibited Use	4
7	Software, Apps & Integrations	5
8	Use of Personal Devices (BYOD)	5
9	Internet, Wi-Fi & Remote Working.....	6
10	Data Handling & GDPR Compliance	6
11	Cyber Security Responsibilities	8
12	Monitoring & Audit Logging	8
13	Termination of Access	8
14	Violations & Disciplinary Action	8
15	Policy Review	9
	Appendix 1: EFH IT Use Policy — Staff Quick Guide.....	10

1 Purpose

This policy governs the **acceptable use of Elizabeth Finn Home's cloud-based systems** (SaaS applications) to support operations, including but not limited to:

- Microsoft 365
- Camascope
- Nourish Better Care
- Xledger
- CareHQ
- Sona & Sona Engagement
- Florence
- ADP iHCM2
- Talos360
- Virtual College

This policy ensures compliance with:

- NHS Data Security & Protection Toolkit (DSPT)
- Care Quality Commission (CQC) – Safe, Effective & Well-Led
- UK GDPR and Data Protection Act 2018
- Cyber Essentials & Cyber Essentials Plus

2 Scope

This policy applies to:

- All employees, agency staff, volunteers, contractors and consultants.
- All devices accessing EFH cloud services (EFH-owned or authorised personal devices).
- All information created, processed, or stored whilst delivering care or business functions.

3 Definitions

- **SaaS application:** A Software-as-a-Service (SaaS) platform is a cloud-based software application that is hosted, maintained, and updated by an external provider, and accessed by users over the internet through a web browser or mobile app.

- **Multi Factor Authentication (MFA):** Multi-Factor Authentication (MFA) is a security process that requires a user to provide two or more independent forms of verification before gaining access to a system, application, or account. It strengthens security because even if a password is stolen, the attacker still cannot log in without the additional verification step.
- **Bring Your Own Device (BYOD):** BYOD is a policy or practice where employees are allowed (or required) to use their personal devices — such as smartphones, tablets, or laptops — to access work systems, applications, email, or data.
- **Phishing:** is a scam that tries to trick you into giving away information or access by pretending to be something legitimate. Common types of phishing include:
 - Email phishing – fake emails designed to steal credentials.
 - Spear phishing and whaling attacks – highly targeted, personalised attack on a specific individual (e.g., CEO impersonation).
 - Smishing – phishing via SMS.
 - Vishing – phishing via voice calls.
 - Clone phishing – attacker recreates a real email with a malicious link.
 - MFA fatigue attacks – repeatedly sending MFA prompts hoping the victim approves.

4 Cloud System Access & Identity Security

- User Accounts
 - Access to cloud systems must use **unique user accounts**, not shared accounts.
 - Multi-Factor Authentication (MFA) is mandatory in any system that supports it.
 - Users are accountable for all actions taken using their credentials.
- Users must not:
 - Share passwords or authentication codes.
 - Allow anyone to use their login, including colleagues, agency staff, or external partners.
 - Save passwords in browsers unless approved by IT.
 - Disable MFA or any security controls.

- Line Manager Responsibilities

Managers must ensure colleague access:

- Matches job role requirements.
- Is removed immediately when no longer required (role change, long-term absence or leaving EFH, etc.).

5 Acceptable Use of Cloud Applications

Cloud applications may be used for:

- Delivery of care (Camascope and Nourish Better Care).
- Finance functions such as Accounts Payable/Receivable (Xledger).
- CRM and billing (CareHQ).
- Rostering, attendance and staff engagement (Sona).
- Payroll, HR, and recruitment (ADP, Talos360).
- Internal communication and file management (Microsoft 365 including NHS email).
- Online training (Virtual College)

Other permitted supplementary applications include:

- SmallPDF,
- Signable
- Signin App
- Boxphish
- ChatGPT (refer to separate Artificial Intelligence (AI) Tools Use Policy)

6 Prohibited Use

Users must not:

- Download or store EFH data outside approved systems.
- Extract sensitive resident or staff data into personal storage (e.g., personal OneDrive, Gmail, WhatsApp).
- Share links or documents externally without managerial approval.
- Use cloud tools and social media to express personal views about EFH or residents.
- Upload malicious or unapproved files into cloud systems.

Examples of Unapproved/Prohibited apps:

- **Personal Cloud Storage Platform:** EFH does not have organisational oversight, data stored outside UK, unapproved encryption standards and risks of accidental sharing. This includes but not limited to:
 - Dropbox
 - Google Drive
 - Google Docs
 - iCloud Drive
 - Amazon Drive

- **Personal Messaging or Communication Apps:** Data cannot be audited, backed up or deleted in line with the EFH retention policy. There is also a high risk of data leakage.
 - WhatsApp (including WhatsApp Web)
 - Facebook Messenger
 - Instagram direct messages
 - Snapchat
 - Telegram
 - Signal
 - WeChat
 - SMS texting for resident/staff data
 - Slack (personal/free workspace)

7 Software, Apps & Integrations

Users must not:

- Install cloud apps without IT approval.
- Connect EFH systems to third-party apps (e.g., Zapier, ChatGPT, Google Drive).
- Enable automatic backups to personal accounts.

8 Use of Personal Devices (BYOD)

- Authorised personal devices may access:
 - Microsoft 365 (via secure app or browser with MFA)
 - Sona mobile app
- BYOD requirements:
 - Devices must have a PIN/password or biometric lock.
 - Devices must support remote wipe (Intune App Protection Policies).
 - No EFH data may be permanently stored on the device.
 - Lost devices must be reported immediately to IT.
- Unauthorized BYOD practices:
 - Accessing cloud systems without a passcode.
 - Screenshotting sensitive data.
 - Syncing work email to unapproved mail apps. Only use Outlook mobile app for work emails.

9 Internet, Wi-Fi & Remote Working

- There are two Wi-Fi networks at each home – **EFHL Staff** and **Elizabeth Finn**
 - EFH Staff Wi-Fi may only be used by approved staff devices.
 - Public Wi-Fi (Elizabeth Finn Wi-Fi) at care homes must **not** be used for work.
- Working Off-site

When working remotely:

- Use company devices where possible.
- Only access cloud systems via secure authentication such as MFA.
- Do not download or export data onto home equipment.

10 Data Handling & GDPR Compliance

- Storage of Data
 - All EFH data must be stored in **approved platforms** as per Section 5 Acceptable Use of Cloud Applications.
 - Data must **not** be stored locally on personal devices, USB/thumb drives, or non-approved cloud services (Dropbox, iCloud, Google Drive).
 - Personal devices may only be used under the **EFH BYOD rules** as per Section 8 Use of Personal Devices (BYOD).

- Accessing Personal Data

Users must:

- Only access the minimum personal/resident data required for their role.
- Not print cloud data unless strictly necessary.
- Dispose of printed data using confidential waste bins.
- Not remove documents containing personal information from the service.

- Sending Sensitive Data

Sensitive or personal data must not be:

- Sent via personal email accounts.
- Shared via WhatsApp, SMS, or other unauthorised messaging platforms.

If sending externally:

- Use secure email (MS365 encrypted mail either from elizabethfinn.co.uk or nhs.net).
- Always confirm the recipient's identity.

10.1 Use of Microsoft 365

- Teams & SharePoint
 - Teams' channels and SharePoint sites must be used for internal collaboration.
 - External sharing requires IT or manager approval.
- OneDrive
 - EFH OneDrive may be used for temporary personal working files.
 - Long-term or team data must be stored in SharePoint or Teams.

- Email

Users must not:

- Forward EFH emails to personal accounts.
- Use Outlook rules to auto-forward mail externally.
- Send unencrypted sensitive information.

10.2 Use of Other Systems

- Nourish Better Care and Camascope (Care and medication records)
 - Care notes must be recorded in Nourish and Camascope in real time, and not written on personal notes, phones, or non-EFH systems.
 - Staff must lock shared terminals/devices when unattended.
- Sona (Rostering & T&A)
 - Staff must not share login details to clock-in or clock-out.
 - Staff must enable location information while using the Sona mobile app.
- CareHQ, Xledger, ADP, Talos360
 - Financial, payroll, and recruitment information is confidential.
 - Reports must not be exported unless necessary and approved.
- Artificial Intelligence (AI) Tools
 - Personal data must not be entered into AI tools
 - AI must not replace professional judgement in care planning or critical decision-making
 - AI outputs must only be used by a member of staff who is a subject matter expert about the output
 - Refer to **Artificial Intelligence (AI) Tools Use Policy** for more information.

11 Cyber Security Responsibilities

Users must:

- Report phishing attempts immediately to the [Data Protection Lead](#).
- Complete mandatory cyber and data protection training.
- Only open links or attachments from trusted sources.
- Not disable antivirus, Intune policies, or mobile app protections.

Compromised or suspicious activity must be [reported to IT immediately](#).

12 Monitoring & Audit Logging

To comply with NHS DSPT & legislative requirements:

- EFH monitors usage of cloud systems, logs security events, and audits high-risk activity.
- Monitoring may include access logs, downloads, email metadata, login behaviour, and file sharing.
- Monitoring is conducted lawfully under UK GDPR regulations.

Users **should not expect their activity to be private**. The organisation may monitor, log, review, or audit usage for legitimate business, security, or compliance purposes.

13 Termination of Access

Upon leaving employment:

- All cloud access will be removed immediately.
- All EFH data must be returned or deleted from any temporary storage.
- Users must not retain or copy work-related data.

14 Violations & Disciplinary Action

Policy violations may result in:

- Suspension or withdrawal of system access.
- Disciplinary action up to and including dismissal.
- Referral to regulatory authorities where required.
- Reporting to the ICO in the case of GDPR breaches.

15 Policy Review

This policy will be reviewed at least annually, or sooner if:

- There are significant changes in relevant legislation or regulatory guidance.
- New technologies or use cases are introduced.
- An incident or audit finding suggests that changes are necessary.

Appendices

Appendix 1: EFH IT Use Policy — Staff Quick Guide

This guide explains how to use EFH's cloud systems safely — including Microsoft 365, Access, CareHQ, Sona, Xledger, ADP, and other online apps.

KEEP YOUR ACCOUNT SECURE

- Always use your own login — never share passwords.
 - MFA (Multi-Factor Authentication) must be used if prompted.
 - Lock your screen when leaving a device.
 - Report suspicious emails or login alerts immediately.
-

USE ONLY APPROVED CLOUD APPS

Approved:

- Microsoft 365 (Teams, Outlook, OneDrive, SharePoint)
- CareHQ, Sona, Xledger, ADP, Talos360
- Any app installed by EFH IT

Not approved:

- WhatsApp, Facebook Messenger, Telegram, Signal
- Dropbox, Google Drive, iCloud, WeTransfer
- Personal email accounts (Gmail, Yahoo, Hotmail)

If unsure, ask IT first.

HANDLING RESIDENT & STAFF INFORMATION

- Keep information inside approved systems.
 - Don't download or save files to personal devices.
 - Don't screenshot, copy or share care/HR information outside EFH systems.
 - Print only when absolutely necessary and dispose in confidential waste.
-

USING DEVICES (EFH-ISSUED OR PERSONAL)

EFH-issued devices

- Don't install your own apps.
- Don't turn off antivirus or security settings.

Personal devices (BYOD) - these are only allowed if:

- Approved by IT
- Protected with a PIN/biometric lock
- Using Microsoft 365 or Sona via secure app/browser
- No EFH files are stored permanently on the device

Lost or stolen personal devices must be reported immediately.

WORKING ON-SITE OR OFF-SITE

- Use **EFH OR Turn2us network** only for work.
 - Do NOT use public Wi-Fi for care information unless on a secure connection.
 - Never leave devices unattended in cars or public areas.
-

EMAIL & TEAMS

- Use EFH email for work only.
 - Do not forward work email to personal accounts.
 - Be careful with links and attachments — when in doubt, don't open it.
 - Use M365 Outlook, Teams/SharePoint to share files, **not** WhatsApp or SMS.
-

MONITORING & SAFETY

- EFH may monitor system use to keep residents, staff, and data safe.
 - This includes logins, file activity, and email security checks.
 - Monitoring is carried out lawfully and respectfully.
-

REPORT ISSUES STRAIGHT AWAY

Tell your manager or IT/Data Protection Lead if:

- You clicked on a suspicious link
- You think your account is compromised
- A device is lost, stolen, or damaged
- You think a data breach may have occurred

Contact: [Data Protection Lead](#) via email.

YOUR RESPONSIBILITY

All staff must follow this guidance to protect:

- resident information
- staff information
- EFH systems and reputation
- compliance with GDPR, CQC, DSPT, and Cyber Essentials