

Elizabeth Finn Homes Limited

Artificial Intelligence (AI) Tools Use Policy

Owner:	Head of IT
Approved by:	Executive Leadership Team (ELT)
Effective from:	January 2026
Review date:	January 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	Principles for AI Use	3
5	Acceptable Uses of AI	4
6	Prohibited Uses of AI	6
7	Roles and Responsibilities	7
8	Approval and Procurement of AI Tools.....	8
9	Data Protection and Privacy	8
10	Incident Management and Reporting.....	9
11	Monitoring and Compliance	9
12	Policy Review	10
	Appendix 1: AI Principles in Practice	11
	Appendix 2: Practical Examples for Care Home Staff	14

1 Purpose

This policy sets out how Artificial Intelligence (AI) tools may be used within Elizabeth Finn Homes to:

- Improve quality and safety of care for residents.
- Support staff in delivering person-centred care.
- Protect residents', relatives' and staff data and privacy.
- Comply with legal, regulatory and contractual requirements, including:
 - UK GDPR and Data Protection Act 2018
 - CQC regulations and guidance
 - NHS Data Security and Protection Toolkit (where applicable)
 - ICO guidance on AI and data protection
 - Employment law and people management policies

It is intended to ensure AI is used responsibly, transparently and safely.

2 Scope

This policy applies to:

- All employees, agency staff, volunteers, contractors, consultants and volunteers.
- All AI tools, systems and services used in a work context, including:
 - Cloud-based AI assistants (e.g. chatbots, document drafting tools).
 - AI embedded in existing systems (e.g. rostering, HR, finance).
 - AI features within Microsoft 365 or similar platforms.
 - AI used for research, analysis, process improvement or training.

3 Definitions

- **Artificial Intelligence (AI):** Technologies that can perform tasks commonly associated with human intelligence, such as recognising patterns, making predictions, generating content or summarising information.
- **Generative AI:** AI systems that can create new content (text, audio, images, video or code) based on prompts.
- **Personal data:** Any information that relates to an identified or identifiable individual (e.g. resident, relative, staff member).
- **Special category data:** Sensitive information that relates to an identified or identifiable individual including:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification)
- Health data (physical or mental health data, diagnoses, treatment, care plans)
- Sex life
- Sexual orientation

4 Principles for AI Use

AI use at Elizabeth Finn Homes must follow these principles. Refer to Appendix 1: AI Principles in Practice for additional information.

- Safety and Quality of Care
 - AI must never replace professional judgement in care planning or clinical decision-making.
 - Residents' safety, dignity and wellbeing always take priority over convenience or efficiency.
- Human Oversight
 - AI outputs must only be used by a member of staff who is a subject matter expert about the output.
 - AI output will only be used to support, not replace, decision-making.
- Lawfulness, Fairness and Transparency
 - AI use must have a lawful basis under UK GDPR.
 - Residents, staff and other data subjects must be informed when their data is processed by AI, where applicable.
 - Data Protection Impact Assessments (DPIAs) must be carried out where AI processing is likely to be high-risk.
- Data Minimisation and Confidentiality
 - Only the minimum data necessary should be input into AI tools.
 - Personal and special category data must not be entered into consumer AI tools.
- Accuracy and Accountability

- AI outputs can be incorrect or biased. Staff must check for accuracy and fairness.
 - Managers remain accountable for decisions where AI tools were used.
- Ethics and Non-Discrimination
 - AI must not be used in ways that discriminate against any individual or group.
 - Models that influence important decisions (e.g. recruitment, rostering) must be reviewed regularly for fairness.

5 Acceptable Uses of AI

When approved by Elizabeth Finn Homes, appropriate examples include:

- Drafting and editing non-confidential documents (e.g. policies, procedures, posters, generic training materials).
- Summarising long policy documents, guidance, meeting notes or research papers that do not include personal data.
- Generating ideas for staff training, wellbeing initiatives or communication campaigns.
- Assisting with internal process mapping, project planning and checklists (without personal data).
- AI features within approved systems (e.g. rostering optimisation, predictive staffing models, call-routing in telephony) where data protection and procurement checks have been completed.
- Supporting accessibility, e.g. translation, converting text into plain language or alternative formats.
- Draft a generic staff newsletter, e.g. about infection prevention (and then editing it before sending).
- Summarise a long CQC or NICE guidance document for internal discussion.
- Generate ideas for a staff or relative events such as a staff wellbeing week or a relatives' information evening.
- Help rephrase internal emails into clearer, plain English (without including personal data).

All such use must be:

- Transparent to colleagues and managers.
- Checked for accuracy, tone and appropriateness.

- Consistent with other organisational policies (e.g. people management, safeguarding, data protection)

.

6 Prohibited Uses of AI

The following are **not permitted** unless explicitly authorised by the Executive Leadership Team (ELT), Data Protection Lead (DPL) / Caldicott Guardian, following a DPIA and appropriate contracts:

Prohibited uses of AI	Examples
Entering personal or resident-identifiable data into unapproved tools	- Names, addresses, dates of birth, NHS numbers. - Health or care information, medication, diagnoses, behavioural notes. - Financial details, bank information, funding status. - Staff performance data, disciplinary records or HR files. Example: Copying and pasting a resident's full care plan or daily notes (with name and medical details) into an online AI chatbot to "summarise it."
Automated or AI-only decisions with significant effect	- Making or heavily influencing admission, discharge or care plan decisions. - Making recruitment, promotion, performance management or disciplinary decisions without human oversight. Example: Using an AI tool to rank job applicants without HR oversight and without checking for bias or fairness.
Surveillance and Monitoring	Using AI (e.g. facial recognition, sentiment analysis) to monitor residents or staff in a way that is intrusive, disproportionate or not legally justified.
Deceptive Use	- Presenting AI content (e.g. messages, emails, letters) as if it were written personally when it has not been reviewed and approved. - Using AI-generated images or audio that could mislead residents, relatives or regulators. Example: Generating a letter to a resident's family using AI and sending it without reading or checking it first.
Bypassing Controls	Using personal devices or unapproved apps to process work information or resident data through AI. Example: Uploading staff HR files to a personal AI account to "help with appraisal writing."

7 Roles and Responsibilities

- Board / Executive Leadership Team (ELT)
 - Approve this policy and set the strategic direction for AI use.
 - Ensure adequate resources for safe, compliant AI adoption.
- Senior Management Team (SMT) / Home Managers
 - Ensure staff in each home understand and follow this policy.
 - Approve local use cases and escalate higher-risk proposals.
- Data Protection Officer (DPO) / Caldicott Guardian
 - Provide advice on lawful use of AI and data protection compliance.
 - Lead or oversee Data Protection Impact Assessments (DPIA) for high-risk AI projects.
 - Liaise with regulators where necessary.
- IT / Information Governance
 - Assess the security, technical and contractual suitability of AI tools.
 - Maintain an inventory of approved AI systems.
 - Monitor usage patterns for security incidents and policy breaches.
- People Team
 - Ensure AI used in recruitment, performance management or HR analytics is fair and transparent.
 - Reflect this policy in people management processes and training.
- All Staff and Volunteers
 - Use AI responsibly and only within the boundaries of this policy.
 - Immediately report any suspected AI-related incident, data breach or harmful output.
 - Undertake mandatory training on AI and data protection.

8 Approval and Procurement of AI Tools

Before a new AI tool is used, the following must be completed/considered:

- Business Case
 - The sponsor (e.g. Home Manager, Head of Department) must define the purpose, benefits, and risks.
- Data Protection and Privacy
 - Identify what data will be processed and whether it includes personal or special category data.
 - Undertake a DPIA where required.
 - Confirm lawful basis and transparency measures (e.g. privacy notices).
- Information Security
 - IT must assess supplier security controls (encryption, access controls, certifications).
 - Confirm data hosting locations and cross-border transfers.
- Contracts and Compliance
 - Ensure appropriate Data Processing Agreements are in place.
 - Check alignment with CQC expectations, NHS DSPT requirements (if applicable) and ICO guidance.
- Pilot and Review
 - Where appropriate, run a small-scale pilot.
 - Evaluate impact, accuracy, user feedback and any incidents, then decide on roll-out.

Only tools approved via this process may be used for resident, staff or business-critical data.

9 Data Protection and Privacy

- AI processing of personal data must comply with UK GDPR principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability).
- Special category data (e.g. health) requires an appropriate legal condition in addition to a lawful basis.

- Where AI is used in ways that are likely to result in high risk to individuals (e.g. profiling), a DPIA is mandatory.
- Data retention for AI outputs and logs must follow the Personal Data Retention & Destruction Policy.
- Individuals' rights (access, rectification, erasure, restriction, objection) must be respected in relation to AI systems.

10 Incident Management and Reporting

AI-related incidents include (but are not limited to):

- Personal data being entered into an unapproved AI tool.
- AI tools producing harmful, discriminatory or clearly inaccurate outputs that could affect residents or staff.
- Unauthorised access, data breach or suspected security compromise involving an AI system.
- Misuse of AI to harass, bully or intimidate staff, residents or relatives (e.g. using AI to generate abusive messages).

If an incident occurs:

1. Report it immediately via email to the [Data Protection Lead](#) (DPL).
2. IT / DPL will assess, contain and investigate.
3. Where necessary, the organisation will:
 - Notify affected individuals.
 - Report to the ICO and/or CQC if required.
 - Document the incident and lessons learned.

11 Monitoring and Compliance

- Elizabeth Finn Homes may review AI usage logs, access logs and system reports to ensure compliance with this policy.
- Non-compliance may result in:
 - Additional training and supervision.
 - Removal of access to specific tools or systems.
 - Disciplinary action in line with people management policies, where appropriate.

12 Policy Review

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

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

Appendices

Appendix 1: AI Principles in Practice

Making safe, ethical, and compliant use of AI in everyday care

ALWAYS PRIORITISE RESIDENT SAFETY

What this means in practice:

- AI can *support* care – it must *never* replace professional judgement.
- Never follow AI-generated suggestions blindly.
- If an AI output looks wrong, unsafe, or unfair → **stop and escalate to a senior.**

Examples

✓ AI suggests rephrasing a care note → check and review before saving

✗ AI recommends a medication schedule → **not allowed**, must rely on clinician instructions.

KEEP PERSONAL DATA SAFE AND MINIMISE WHAT YOU SHARE

What this means for you:

- Do **not** enter resident names, medical details, relatives' information, safeguarding notes, or staff information into *any* AI tool unless approved for that purpose.
- For general tasks (emails, posters, summaries), remove names and private details.

Examples

✓ “Summarise this long CQC regulation”

✗ “Summarise this resident’s care plan”

✗ “Write a message to David Smith’s daughter about his medication change”

ALWAYS REVIEW AND EDIT AI OUTPUTS

AI can make mistakes (“hallucinations”). You are responsible for correcting them.

What this means in practice:

- Always proofread AI-generated text before using it.

- Check spelling of names, dates, shifts, or policies.
- Ensure tone is appropriate and aligned with care values.

Examples

- ✓ Using AI to draft a poster for a staff wellbeing event—check it before sharing
 - ✗ Sending an AI-generated relatives' letter without reading it first
-

USE ONLY APPROVED AI TOOLS

Why: Approved tools have been checked for data security, UK GDPR compliance, and Data Security and Protection Toolkit (DSPT) requirements.

What this means:

- Use the AI features inside approved systems:
 - Microsoft 365 / Copilot / Teams Premium (note taking)
 - Sona (rostering) AI features (if enabled)
- Avoid “free” AI websites or mobile apps unless explicitly authorised.

Examples

- ✓ Using Copilot to draft a meeting summary (without resident data)
 - ✗ Uploading staff rotas to an unapproved AI website to “make it nicer”
-

BE TRANSPARENT AND HONEST

What this means:

- Residents, relatives, and colleagues must not be misled.
- When AI helps produce a document (poster, message, report), it should still be reviewed and issued by a real person.

Examples

- ✓ “I used a tool to help draft this, but I have checked it.”
 - ✗ Pretending that an AI-created letter is personally written when it hasn't been reviewed
-

BE FAIR AND WATCH FOR BIAS

AI can unintentionally treat people differently.

What to look out for:

- Does the AI suggestion disadvantage any resident?
- Does it make an assumption based on age, disability, ethnicity, or diagnosis?

Examples

✓ Checking shift suggestions to ensure fairness across staff

✗ Allowing an AI-generated recruitment summary to influence hiring without this being reviewed

KNOW WHEN TO ESCALATE

Tell a manager or the Duty Manager if:

- AI output seems unsafe, inappropriate, discriminatory, or inaccurate
- You accidentally entered resident or staff data into an unapproved AI tool
- The AI system behaves strangely (missing data, odd results, wrong suggestions)

This is treated like any **information governance incident** or **clinical risk**.

APPLY THE “CARE HOME TEST”

Before using AI for anything, ask yourself:

- Would I be comfortable explaining this to the resident or their relative?
- Am I protecting their dignity, privacy, and confidentiality?
- Am I still making the final decision—not the AI?
- Would I be happy for this to be reviewed by the DPO, CQC, or ICO?

If the answer to any is **no**, do not use the AI for that task.

Appendix 2: Practical Examples for Care Home Staff

Good, Safe Use Cases

- ✓ Drafting a staff newsletter (no personal data)
 - ✓ Summarising a long policy or guidance document
 - ✓ Creating ideas for activities, events, or menus
 - ✓ Rewriting a message to make it clearer
 - ✓ Helping produce a checklist for a process (e.g. onboarding new staff)
 - ✓ Drafting generic training materials
 - ✓ Improving grammar in reports that contain NO identifiable data
-

Use Cases That Require Approval

- ⚠ AI for rostering optimisation
 - ⚠ AI that analyses CCTV or movement data
 - ⚠ AI used for recruitment ranking or staff performance insights
 - ⚠ AI embedded in clinical or medication systems (needs clinical safety review)
-

Prohibited Use Cases (Not Allowed)

- ✗ Entering care notes, charts, diagnoses, personal or medical details into AI tools
- ✗ Uploading photos of residents into apps without consent and approval
- ✗ Using AI to write care plans or risk assessments
- ✗ Using AI for clinical or medication decisions
- ✗ Using AI to monitor staff behaviour or productivity
- ✗ Creating messages that could be harmful, bullying, or misleading