Title of Document	**Artificial Intelligence Policy**
Name of Department	**TechTeam**

What type of document is this?	**Policy**		
Which Helping Hands POL/SOP/W.I does this document relate to?	N/A	**Reference number of POL/SOP/W.I**	N/A

Which Operational Priority/Priorities does this document link to?	Governance Framework	Information Management & Technology		

Custodian of document	Chief Financial Officer	**Committee/Group responsible for this document**	Policy Committee
Approval date and committee chairperson signature	30.05.25	**When is its next scheduled review?**	30.05.26

Who does it apply to?	All staff at the facility, All 3rd party partners				
	Does it apply to bank workers?	Yes	**Does it apply to agency staff?**	Yes	**Does it apply to third party contractors?**	Yes

Purpose of the Policy	This policy outlines the principles and guidelines for the ethical, secure, and effective use of Artificial Intelligence (AI) technologies at Helping Hands Home Care. It ensures compliance with UK regulations, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, while enhancing care delivery through AI.

Summary of Key POL Requirements

ROLES AND RESPONSIBILITIES

Role	Responsibility
IT Director	Champion the ethical, secure, and effective use of AI. Monitor updates to AI-related regulations and ensure the organisation adapts. Allocate resources for compliance and improvement of AI systems.
Head of Digital	Embed this AI Policy within digital content creation and marketing. Monitor AI use in content generation (e.g. social media or website) for compliance and accuracy.
Head of Service Delivery	Embed this policy within operational teams (TechTeam and Care teams). Monitor AI usage in Service Delivery, and promptly escalate any AI-related risks or concerns. Ensure staff are trained in AI tools used for care.
DPO	Oversee data protection compliance for all AI initiatives. Ensure DPIAs are completed and privacy controls are in place. Advise on lawful bases for AI data processing and liaise with regulators (ICO, etc.) as needed.
Ethical Review Board / AI Governance Committee	Review and approve new high-risk AI projects before deployment (see section 9.0). Provide multidisciplinary oversight (including clinical, technical, and ethical perspectives) for AI system development and use.
All Staff and Contractors	Adhere to this policy in their use of AI. Complete required training on AI ethics and security. **Report any issues, errors, or concerns** related to AI systems immediately (see Incident Reporting at §5.0). Staff must not rely on AI outputs without appropriate verification and must safeguard sensitive data when using AI.

1.0 Scope

This policy applies to all employees and partners who use or interact with AI systems and data at Helping Hands Home Care. It covers AI solutions developed in-house or provided by third parties, including general-purpose AI services (e.g. cloud AI or language models) used in our operations. **Note:** The organisation will not deploy any AI application that is prohibited by law or that poses an unacceptable risk to individuals' rights or safety (such as AI for social scoring or other unethical purposes).

2.0 Ethical Principles

We commit to the following core principles for AI use, consistent with global best practices (e.g. the FUTURE-AI guidelines:

- **2.1 Transparency:** AI use must be transparent and understandable to users and stakeholders. Whenever AI tools (like chatbots or decision aids) interact with staff or clients, we disclose that the interaction is AI-driven. Service users should be aware when AI contributes to their care.

- **2.2 Fairness:** AI algorithms should avoid bias and ensure equitable treatment of all individuals. We strive for **universality** in AI – meaning solutions are inclusive and effective across different patient groups, preventing discrimination against any age, gender, ethnicity, or other demographic. Regular bias assessments will be conducted (see section 12.0).

- **2.3 Accountability:** Clear responsibility must be assigned for management and outcomes of AI systems. Human professionals retain ultimate accountability for decisions supported by AI – AI is a tool to assist, not replace, professional judgment. Any clinical or care decision influenced by AI must be reviewed and approved by qualified staff.

- **2.4 Data Minimisation:** Collect and use only the data necessary for intended AI functions. We follow GDPR principles in limiting personal data and ensure any personal health information is used in line with its original purpose (see §4.0 Data Protection).

- **2.5 Security:** Implement robust security measures to protect data and AI systems from unauthorised access and breaches. This includes cybersecurity safeguards and access controls (see section 6.0).

- **2.6 Human Oversight & Explainability:** AI systems must be subject to appropriate human oversight at all times. Designs should prioritise explainability – results or recommendations should be interpretable so that staff can understand the rationale. No AI will operate as a "black box" for critical decisions without human review.

- **2.7 Robustness:** AI solutions should be robust and reliable. They must be tested for safety under various conditions and have fail-safes or fallback procedures if they

malfunction. We only use AI in care delivery if it has proven accuracy and can maintain performance across different environments.

3.0 Data Protection and Privacy

We treat personal data used in AI systems with the highest care, complying with the UK GDPR, Data Protection Act 2018, and guidance from the ICO:

- **3.1 Lawful Basis & Transparency:** Collect and process personal data for AI in accordance with GDPR principles. A clear purpose for data use must be defined and communicated to individuals. We inform data subjects about what data is collected for AI and why (e.g. to improve care, to assist in decision-making).

- **3.2 Anonymisation:** Where possible, use anonymised or de-identified data in AI systems to protect privacy. For example, patient data used to train an AI model should be de-identified unless real-time personal data is absolutely necessary.

- **3.3 Data Minimisation:** Limit data collection to what is strictly required for the AI's purpose. Avoid using any data in AI that is not relevant to the care or service objective.

- **3.4 Fair and Transparent Processing:** Ensure personal data is processed lawfully, fairly, and transparently. Individuals have the right to know if AI is analysing their data, and how. If AI outputs will inform someone's care, this should be included in privacy notices.

- **3.5 Access Control:** Restrict access to personal data used in AI to authorised personnel only. For AI systems processing health data, access must be role-based and regularly reviewed.

- **3.6 Data Security:** Store personal data used in AI securely, using encryption and other protective measures. Data in transit to/from AI services (e.g. cloud AI APIs) must be encrypted. Any AI models or datasets are stored on secure, approved platforms.

- **3.7 Data Sharing:** Do not share personal data with third-party AI providers without proper agreements and, where required, patient consent. Any data sharing for AI

development (e.g. with a vendor training a model) must undergo legal review and ensure GDPR-compliant safeguards (such as Data Processing Agreements).

- **3.8 Data Protection Impact Assessment (DPIA): Before implementing any new AI system or significant change, a DPIA must be complete** This legal requirement helps identify and minimise risks to individuals. The DPIA should evaluate how the AI will use personal data, risks to privacy or rights, and measures to mitigate those risks. The DPO must sign off on all AI-related DPIAs.

- **3.9 Individual Rights:** Respect individuals' data protection rights in the context of AI. This includes the right to access their data, correct inaccuracies, or object to certain processing. If an AI system uses personal data to make or inform decisions about individuals, mechanisms must be in place to address any data subject requests (e.g. the right to an explanation or to contest an automated decision).

- **3.10 Automated Decisions:** Helping Hands Home Care will **not** rely on solely automated AI decisions that have legal or similarly significant effects on individuals, except in accordance with Article 22 of UK GDPR. In practice, this means any decision affecting a person's care, employment, or services will have human involvement and review. AI may flag issues or provide recommendations, but final decisions rest with human staff (see Accountability in §2.3). Where automated processing is used, individuals will be informed and given the opportunity to request human review of the outcome.

4.0 AI System Development and Use

- **4.1 Ethical AI by Design:** Develop or select AI systems with ethical considerations from the start. We favour AI tools that have been designed for fairness, transparency, and privacy. For in-house projects, incorporate ethics and privacy by design (consult the Ethical Review Board and DPO during development).

- **4.2 Validation and Testing:** Thoroughly test and validate AI systems before deployment to ensure accuracy, efficacy, and reliability. This includes clinical validation for any AI that will support care decisions – e.g. comparing AI recommendations against expert human judgment and known outcomes. Tests must cover diverse scenarios and patient groups to ensure consistent performance.

- **4.3 Monitoring and Auditing:** Continuously monitor AI system performance and conduct regular audits for ethical compliance. Key metrics (e.g. accuracy, error rates, any adverse events) should be tracked. If an AI system's performance drifts or degrades over time, or if biases are detected, immediate action (retraining, tuning, or suspension) must be taken (see §12.0 Bias Mitigation). Audits should be documented and reported to management.

- **4.4 Ownership and Maintenance:** Establish clear ownership for each AI system or tool – assign a system owner responsible for its maintenance and compliance. Ensure AI models and software are kept up to date (applying updates or retraining as needed to maintain accuracy and security). If using third-party AI, confirm the vendor's responsibilities for support and updates over the system's lifecycle.

- **4.5 Documentation and Traceability:** Maintain detailed documentation for AI systems, including their intended use, design/algorithm description, data sources, and testing results. All deployments of AI should be logged for traceabilit Significant interactions or decisions by high-risk AI (e.g. a care recommendation) should be recorded (logged) to enable review and audit of how that outcome was reached.

- **4.6 Procurement and Vendor Standards:** When procuring AI products or services, perform due diligence. Vendors must demonstrate that their AI tools comply with healthcare regulations and this policy. For AI systems that qualify as medical devices (e.g. diagnostic or monitoring algorithms), only use solutions that are properly certified (UKCA or CE marked, or approved by MHRA/FDA as required) and have evidence of clinical safety and efficacy. Vendor contracts should include provisions for algorithm transparency, data protection, and an obligation to report any known issues or updates to their AI.

- **4.7 Generative AI Use:** Generative AI systems (such as large language model chatbots or AI content generators) must be used cautiously in care and administrative settings. Any content produced by generative AI (e.g. draft care notes, recommendations, or communications) should be **reviewed and verified by staff** before it is relied upon or shared. Employees should recognise that generative AI can produce errors or "hallucinations" thus, critical information from such tools must be fact-checked. Generative AI should not be used to provide medical advice to patients without a human clinician validating the information.

5.0 Incident Response and Reporting

- **5.1 Internal Reporting Mechanism:** We have an established mechanism for employees to promptly report any issues, malfunctions, or incidents involving AI systems. This includes potential data breaches, cases of AI providing incorrect or harmful outputs, or any ethical concerns. Such reports should be made to the IT Director, Head of Service Delivery, or via the Cyber and Data Security Incident Response Plan (v1.1) as appropriate. All reports will be reviewed and investigated immediately.

- **5.2 Incident Response Plan:** The organisation will maintain and follow an incident response plan specific to AI-related incidents (in coordination with our general cyber incident response). This plan will detail steps for containing and remediating any AI malfunction or misuse, communicating to affected parties, and learning from the incident to prevent recurrence. For example, if an AI system is found to have made a significant error in a care recommendation, the plan may involve halting the AI's use, informing the care team and patient, and correcting any decision made.

- **5.3 External Incident Reporting:** In line with emerging regulations, Helping Hands will report serious AI-related incidents to relevant authorities when required. If an AI system used in care qualifies as a medical device and it malfunctions or causes harm, we will notify the MHRA (per medical device vigilance rules). If an AI-related data breach or privacy violation occurs, we will report to the ICO within statutory timeframes. We will also cooperate with any oversight bodies established under the EU AI Act for reporting "serious incidents or malfunctioning" of high-risk AI. All such reports and communications will be coordinated by the DPO and IT Director.

6.0 Security Measures

- **6.1 Encryption:** Use strong encryption to protect personal and sensitive data used by AI, both at rest and in transit. For instance, any databases of care records used by an AI are encrypted, and any network communication between our systems and an AI service (including cloud APIs for AI) must use encryption (HTTPS/TLS).

- **6.2 Access Control:** Implement strict access controls for AI systems and the data they use. Only authorised individuals can run or input data into high-risk AI tools. Access is granted based on least privilege and needs regular review. If an AI system has an administrative interface, it must be protected with strong authentication and audit logging of administrator actions.

- **6.3 Incident Preparedness:** Maintain up-to-date security measures and an incident response capability (see §6.0) to promptly address any security breaches or AI misuse. Conduct periodic penetration testing or security assessments of AI infrastructure to identify vulnerabilities.

- **6.4 Regular Updates:** Keep AI software, libraries, and platforms updated to patch security vulnerabilities. If using third-party AI services, stay informed of their security announcements. Decommission or upgrade AI systems that cannot meet current security standards.

- **6.5 Physical Security:** Ensure that any hardware used for AI (servers, IoT devices in homecare, etc.) is secured against theft or tampering, especially if they store personal data or run critical AI functions.

7.0 Training and Awareness

- **7.1 Employee Training:** Provide regular training to employees on AI ethics, data protection, and security best practices. Training modules will include real-world examples of AI benefits and risks, recent incidents or legal cases to illustrate consequences of misuse, and guidelines on how to appropriately interpret AI outputs. New staff must complete AI policy training as part of induction.

- **7.2 Awareness Programs:** Conduct ongoing awareness campaigns to inform both internal and external stakeholders about our use of AI and its limitations. For staff, this includes updates when new AI tools are introduced (covering how to use them properly and pitfalls to avoid). For clients or patients, we will communicate, where relevant, how AI assists in their care (for example, explaining an AI-driven fall detection system to a homecare client and its known limits).

- **7.3 Specialised Workshops:** Organise periodic workshops or drills for teams using AI in critical processes (such as clinical decision support or medication management). These workshops will reinforce skills in validating AI output, managing AI errors, and protecting patient data when using AI.

- **7.4 Policy Accessibility:** Ensure the AI Policy (this document) is easily accessible to all staff (e.g. on the intranet). Encourage staff to refer to it whenever planning a new project involving AI or if they have questions about proper AI use. Management will

highlight key policy points at team meetings especially when new relevant laws or guidelines come into effect.

8.0 Compliance and Legal Reviews

- **8.1 Compliance Checks:** We will regularly review and update this AI Policy to ensure compliance with all relevant laws, regulations, and standards. This includes monitoring developments in the **EU AI Act**, UK laws and regulatory guidance, and any industry standards for AI in healthcare. For example, as the EU AI Act moves toward full applicability by 2026, we will align our high-risk AI practices (e.g. for any diagnostic AI) with its requirements (risk assessments, documentation, human oversight, etc.).

- **8.2 Regulatory Developments:** A formal review will occur at least annually (or sooner if major regulation changes occur). The IT Director (or designated AI Governance lead) will track emerging rules like **the European Commission's GPAI (General-Purpose AI) guidelines**, any new UK legislation or NHS guidance, and rulings/enforcement by bodies like the ICO. The policy will be amended as needed and changes communicated to staff.

- **8.3 Ongoing Legal Oversight:** Engage legal counsel or compliance officers to conduct regular reviews of our AI use for any emerging legal risks. This may include ensuring our AI-driven processes do not inadvertently violate discrimination laws, employment laws, or medical regulations.

- **8.4 External Audits:** If required by law or best practice, we will subject our AI systems to external audit or assessment. For instance, high-risk AI used in care might be audited for compliance with the NHS AI governance standards or certification requirements. Any recommendations from such audits will be addressed in a timely manner.

9.0 Ethical Review Board

- **9.1 Establishment:** An **Ethical Review Board (ERB)** or similar governance committee is in place to oversee the ethical development and deployment of AI systems at Helping Hands. This Board includes senior management, the DPO, clinical

representatives, and subject matter experts in AI. Its mandate is to ensure that any AI project aligns with our ethical principles and regulatory obligations.

- **9.2 Review Process:** The ERB will conduct formal reviews of proposed new AI technologies or significant upgrades. The process will evaluate the project's purpose, data usage, potential biases, risk of harm, and mitigation plans. Ethical implications are documented and discussed. The ERB may use external guidelines (like the National Academy of Medicine's framework for generative AI oversight) as reference to gauge if we are adequately addressing risk versus benefit.

- **9.3 Approval Mechanism:** ERB approval is required **before deploying any new AI system** that impacts care delivery or processes sensitive personal data. The Board can mandate changes or additional safeguards as a condition of approval. For lower-risk AI (e.g. administrative efficiency tools), a lighter review may be done by the DPO/IT governance team. No AI with unresolved ethical or legal concerns will move forward.

- **9.4 Continuous Oversight:** The ERB (or a designated AI oversight group) will also periodically review ongoing AI uses. This includes examining audit reports, incident reports, and new evidence. The Board has authority to suspend or withdraw an AI tool from use if ethical or safety issues emerge.

10.0 Continuous Improvement and Feedback Loop

- **10.1 Feedback Collection:** Establish a feedback loop to gather input from employees, clients, and other stakeholders on their experience with AI systems. For example, care staff using an AI scheduling assistant can provide feedback on its usability or any concerns, and clients can be surveyed about their comfort and trust in any AI-supported services.

- **10.2 Learning from Feedback:** Use feedback and real-world data to drive improvements. If staff report that an AI tool's recommendations are occasionally inappropriate, we feed this information back to developers or vendors for refinement. We encourage a culture where constructive criticism of AI tools is welcomed as a means to improve them.

- **10.3 Policy Iteration:** Regularly review this policy itself to ensure it remains effective and relevant. Incorporate lessons learned from incidents (as noted in §6.0) or from new best-practice frameworks. For instance, incorporate any future consensus

guidelines from healthcare authorities or international standards (ISO, etc.) that may emerge. Version updates will be clearly documented (see change log) and communicated.

11.0 Bias Mitigation Strategy

- **11.1 Bias Audits:** Regularly conduct audits to identify any unintended bias in AI systems. This involves reviewing AI outcomes for different groups of service users. For example, if an AI risk scoring system is used to prioritise home visits, we will check that it does not systematically undervalue any group (such as older adults or minorities). Bias audit results shall be reported to the Ethical Review Board and used to guide retraining or recalibration of models.

- **11.2 Remediation Plans:** If biases are detected, implement prompt remediation. This could include retraining the AI with more diverse data, adjusting algorithm parameters, or in some cases discontinuing use of the AI until fixed. The remediation plan will assign responsibility and timeline for bias reduction, and the effectiveness of these actions will be evaluated in follow-up audits.

- **11.3 Inclusive Design:** Strive for inclusive design of AI solutions from the outset – meaning consider the needs of diverse user groups in development. Solicit input from a range of stakeholders (e.g. patients with different backgrounds) when designing or selecting AI, to pre-empt bias. Document how training data was collected and ensure it's representative of our client population where feasible.

12.0 Risk Assessment Procedures

- **12.1 Risk Assessments:** Conduct thorough risk assessments before deploying any new AI system, in addition to the DPIA noted in §4.8. These assessments evaluate ethical, legal, clinical, and operational risks. We use a structured approach (following frameworks like the NIST AI Risk Management Framework or NHS AI risk templates) to rate risks (e.g. patient safety risk, data risk, reputational risk) and define mitigation strategies.
- **12.2 Ongoing Risk Management:** Maintain an AI risk register or hazard log for all active AI systems (aligned with NHS guidance on AI safety cases). Update this register whenever there are changes or when new risks are identified. High residual risks must be reviewed by management and the Ethical Review Board to determine acceptability.

- **12.3 Pre-Deployment Review:** No AI system will be moved into live use without completion of the above risk assessment and sign-off that risks are at an acceptable level or have appropriate controls. For high-impact AI, consider a pilot phase or sandbox testing (as encouraged by regulator to safely evaluate performance in a controlled manner before full rollout.

13.0 Integration with Existing Systems

- **13.1 Seamless Integration:** Ensure AI systems integrate smoothly with existing IT infrastructure and workflows. AI should support and enhance our operations, not disrupt them. Before introduction, test compatibility with our electronic health record systems, care management systems, etc. Provide guidelines or training to staff on how the AI fits into their daily work (e.g. how an AI scheduling assistant works with the current scheduling software).

- **13.2 Minimising Disruption:** Plan deployments to minimise disruptions. For example, introduce AI tools during low-activity periods or run them in parallel with legacy processes until trust is established. Have a rollback plan in case the integration causes issues.

- **13.3 Interoperability Standards:** Prefer AI solutions that adhere to open interoperability standards (where applicable in healthcare, e.g. HL7/FHIR for data) to ensure they can exchange data safely and effectively with our systems. Avoid vendor lock-in that could hinder future integration or export of our data.

- **13.4 Continuous Monitoring of Integration:** After deployment, monitor how well the AI system is integrating. Gather user feedback on any workflow issues. If, for instance, an AI documentation assistant slows down the process or causes confusion, refine the integration (perhaps by adjusting its prompts or when it is invoked).

14.0 Stakeholder Involvement

- **14.1 Stakeholder Engagement:** Involve relevant stakeholders in AI development and deployment phases. This includes not just technical staff, but also caregivers, nurses, clients (or patient representatives), and management. Their insights help ensure the AI addresses real needs and is trusted. For example, if developing an AI fall detection system for homecare, involve some of the caregivers and possibly clients/family members in the design or pilot to get feedback on usability and comfort.

- **14.2 Building Trust:** Communicate openly with stakeholders about the introduction of AI. Highlight the intended benefits (efficiency, improved care outcomes) and the safeguards in place. Allow stakeholders to voice concerns. Trust is crucial: as noted by WHO and others, AI in health will only succeed if people trust it. Transparency and engagement are key to building this trust.

- **14.3 Collaboration and Oversight:** Collaborate with external partners (industry, academia) responsibly. If we partner with a tech company for an AI tool, we ensure our stakeholders' interests (like patient safety and data privacy) are represented in that partnership. We may also participate in sector-wide forums or working groups to share experiences and learn from others on safe AI adoption.

15.0 Data Accuracy and Quality Assurance

- **15.1 Quality of Data:** Implement data quality assurance processes for any data used to train or feed AI systems. Inaccurate or poor-quality data can lead to poor AI outcomes. We will routinely validate datasets (for example, ensuring that health records used for an AI clinical decision tool are accurate and up-to-date). Remove or correct faulty data that could skew AI behaviour.

- **15.2 Verification of Outputs:** Treat AI outputs as advisory unless proven otherwise. Staff must verify critical AI-generated outputs. For instance, if an AI suggests a change in a patient's care plan, a qualified professional should cross-check this recommendation against clinical guidelines or a second opinion. This verification step is part of our quality assurance to catch AI errors before they affect clients.

- **15.3 Continuous Quality Monitoring:** Monitor the quality of AI outputs over time. Set up a schedule (e.g. monthly review of a sample of AI decisions or documents) to ensure they meet our standards. If any decline in quality is observed (perhaps as data drifts or new use cases arise), take corrective action—such as model retraining, rule adjustments, or additional training for users on how to input queries to AI effectively.

- **15.4 Human-in-the-Loop:** Maintain a "human-in-the-loop" for quality control, especially for generative AI applications. For example, if using an AI to draft care visit summaries, a human reviewer should always finalise the report, correcting any mistakes the AI may have made. This not only ensures accuracy but also helps the AI improve (if it's a learning system) by providing feedback.

- **15.5 Logging and Review:** Keep logs of AI outputs and decisions (as mentioned in §5.5) to facilitate retrospective review. If an issue is later found (e.g. an AI misidentified a risk level), we can trace back through logs to understand what input data or logic led to that output. This helps in debugging and improving the system.

16.0 Employee Acceptable Use of AI Platforms

- **16.1 Restricted Information:** Employees are **strictly prohibited** from inputting any sensitive or personal data (especially patient identifiable information) into external AI platforms or tools that are not approved for such use. This includes public generative AI services (e.g. ChatGPT, Google Bard) and any AI tool not authorised by Helping Hands for handling confidential data. For example, an employee must not paste a client's medical details into a free AI chatbot to get advice. Any exception would require explicit written approval from senior management and the DPO, with a clear justification and safeguards.

- **16.2 Use of Approved Tools:** Only use AI platforms that have been vetted and approved by the organisation for specific purposes. For instance, if an AI writing assistant is approved for drafting general communications, it may be used *only* for that purpose and with provided guidelines. All usage must comply with licensing and terms of service of the tool, and no intellectual property or data rights of the organisation should be jeopardised.

- **16.3 Employee Guidance and Awareness:** Employees will receive training on the risks of using AI platforms, emphasising data security and result verification. They should understand that what is input into some AI services could be stored or used to train models (thus the importance of not revealing sensitive info). They are also warned about the possibility of AI-generated content being incorrect or biased.

- **16.4 Output Verification:** Any output obtained from an AI platform by an employee for work purposes must be reviewed for accuracy and appropriateness. The employee is responsible for fact-checking AI-generated text or analyses. Under no circumstances should unverified AI output be directly sent to clients or used in decision-making. For example, if an AI drafting tool writes a letter to a client, the staff member must proofread it thoroughly to ensure it's correct and professional.

- **16.5 Consequences of Violations:** Violations of these acceptable use rules (e.g. an employee uploading a client list to an unauthorised AI service, or acting on faulty AI advice without verification) may result in disciplinary action, up to and including termination of employment. These rules are in place to protect our clients' privacy and safety, and to protect the organisation from legal and reputational harm.

17.0 Compliance and Enforcement

- **17.1 Enforcement:** All managers are responsible for enforcing this policy. Any breach of the policy will be taken seriously. Investigations will be carried out for suspected violations, and appropriate disciplinary measures will be applied where the policy has not been followed. For instance, if an employee knowingly deploys an AI tool without approval or neglects required oversight leading to an incident, that will be addressed under our disciplinary procedures.

- **17.2 Regular Compliance Audits:** We will conduct periodic compliance audits to ensure the policy is being followed (this aligns with §9.1 on compliance checks). This might include checks like: reviewing a sample of AI decisions for proper human sign-off, verifying that DPIAs exist for AI projects, and interviewing staff on their awareness of AI usage rules. Non-compliance issues identified will be rectified with corrective action plans.

- **17.3 Record-Keeping:** Compliance efforts (training records, DPIA documents, audit reports, etc.) will be documented. These records demonstrate our accountability and readiness to show regulators our compliance with AI governance expectations (important under both GDPR and upcoming AI regulations).

- **17.4 Policy Accessibility and Attestation:** This policy will be accessible to all staff. Key staff must attest (electronically or in writing) that they have read and understood the AI Policy, especially when significant updates are made. This attestation may be renewed annually. Ensuring everyone understands and agrees to follow the policy is a part of enforcement.

18.0 Contact Information

For questions or concerns about this AI Policy or any AI-related issue, please contact the **Data Protection Officer (DPO)** or the IT Director:

- **Karyn MacKenzie, Data Protection Officer** – Email: **karyn.mackenzie@helpinghands.co.uk**

- (Alternatively, staff may contact their line manager or the IT helpdesk, who will escalate queries to the appropriate policy custodian.)

TRAINING

Is training required?	Yes
Details of training	Initial training to be provided: • Employee Training • User Awareness Training

COMPLIANCE

How is compliance with the POL going to be monitored	Compliance with Policy will be monitored through the following: • Employee Acceptable Use Policy for AI Platforms • Compliance checks: regularly review and update this policy to ensure compliance with relevant laws and regulation

EQUALITY IMPACT ASSESSMENT AND PROCEDURAL INFORMATION

	Positive / Negative / N/A	Comments
Does the document have a positive or negative impact on one group of people over another on the basis of their:		
• age?	N/A	
• disability?	N/A	
• gender reassignment?	N/A	
• pregnancy and maternity (which includes breastfeeding)?	N/A	
• race (including nationality, ethnic or national origins or colour)?	N/A	
• marriage or civil partnership?	N/A	
• religion or belief?	N/A	
• sex?	N/A	
• sexual orientation?	N/A	

If you have identified any potential impact (including any positive impact which may result in more favourable treatment for one particular group of people over another), are any exceptions valid, legal and/or justifiable?	N/A	
If the impact on one of the above groups is likely to be negative:		
• Can the impact be avoided?	N/A	
• What alternatives are there to achieving the document's aim without the impact?	N/A	
• Can the impact be reduced by taking different action?	N/A	
• Is there an impact on staff, client or someone else's privacy?	N/A	*If yes, privacy impact assessment required*

What was the previous version number of this document?	Version 01	
Changes since previous version	• Established AI Ethics Committee and central AI Inventory. • Added Data Protection Officer role and GDPR-aligned privacy-by-design requirements. • Introduced bias-mitigation strategy, structured risk assessments, and AI incident-response process. • Created employee Acceptable-Use rules for AI platforms (incl. generative AI). • Strengthened security controls (encryption, access, monitoring). • Added transparency & explainability mandates and quarterly performance/bias audits. • Incorporated EU AI Act timelines and latest UK/ICO guidance. • Made DPIAs mandatory before any AI deployment. • Added detailed rules for Generative AI/LLMs (data-input restrictions, output verification). • Strengthened human-oversight clause for all AI-assisted decisions. • Expanded DPO role; clarified clinician accountability. • Required MHRA/medical-device certification for clinical AI tools. • Introduced external incident-reporting requirement to regulators. • Enhanced bias-mitigation audits, safety validation, and vendor contract clauses.	
Who was involved in developing/reviewing /amending the POL?	IT Director Head of Digital	
How confidential is this document?	Restricted	Can be shared freely within Helping Hands but NOT outside

References	
Associated Documents	*Information Security (Inc Cyber Security) Policy*