AI Use Policy

Policy Number	47
Version	1
Policy Contact	Matthew Betteridge
Date Issued	22nd December 2025
Review Date	06th May 2026
Next Review Date	06th May 2027
Target Audience	Employees and Staff
Approved by	OneCall24 Policy Team

1. Purpose

AI tools are becoming more common in healthcare and can make our work faster, easier, and more creative. This policy explains how we can use AI safely, responsibly, and in line with UK GDPR and the Data Protection Act 2018. It also outlines what staff should consider before using any AI or third-party system so that we protect patients, staff, and the organisation.

2. Scope

2.1 Roles Covered:

This policy applies to everyone working for the organisation, including:

- Directors
- Managers and Team Leaders
- Administrative and office staff
- Clinical staff
- Non-Clinical staff
- Temporary, agency, and contracted workers

3. Objectives

- Encourage safe and helpful use of AI in everyday work
- Ensure staff understand safeguards required when using AI or third-party processors
- Comply with UK GDPR and Data Protection Act 2018
- Protect personal data and minimise risk to vulnerable individuals

4. Policy

4.1 Why We Use AI

AI can support staff with drafting, summarising, planning, organising information, and generating ideas. However, AI tools can be inaccurate or biased. Outputs must always be checked. AI should support, not replace, professional or clinical judgment.

Staff remain fully responsible and accountable for any work produced using AI tools.

4.2 Safe Use of AI - Everyday Rules:

Never:

- Enter identifiable patient information into external AI platforms like ChatGPT
- Upload confidential or internal documents into unapproved AI systems
- Use AI to make clinical or safety-critical decisions
- Accept AI outputs without reviewing them carefully

Please Do:

- Use AI for drafting, summarising, planning, and idea generation
- Ask AI to improve wording or format
- Use internal approved AI tools such as Microsoft Copilot
- Review, verify, and edit all AI-generated content
- Seek advice from a Manager or Director before using any AI tools or if you are unsure of your use case.

Use of AI tools may be monitored to ensure compliance with this policy and data protection requirements.

4.3 ChatGPT vs Microsoft Copilot ChatGPT – Strengths and Limitations:

ChatGPT (external tool):

- Great at conversation, writing, generating ideas
- Very flexible and creative
- However: Data isn't private. You must never input personally identifiable client/end user information or confidential information into this tool.

Microsoft Copilot (internal tool):

- Works safely inside our secure Microsoft systems
- Good for summarising internal files, emails, and documents
- Useful for admin and workflow support
- However: Less creative and limited by organisational access permissions and data access rules.

Both tools require staff to verify accuracy of outputs and maintain confidentiality.

4.4 Considering New AI Tools

Before using new AI systems, the organisation will consider:

- Whether it is genuinely needed
- Whether personal data is involved and if its use is appropriate

- Whether a DPIA is required
- Reputation and reliability of the provider
- Risks related to fairness, accuracy, bias, and safety
- Any updates needed to internal processes or privacy notices

No new AI tool may be used until it has been reviewed and approved by the organisation (e.g. IT, Compliance, or Data Protection lead).

4.5 Our Role as Data Controller

OneCall24 is the Data Controller for personal data processed in connection with our services.

This means:

- We decide how and why personal data is used
- We ensure any AI tool or external provider meets GDPR requirements
- We monitor data safety, accuracy, and compliance
- Accountability stays with us, even when external systems are involved

4.6 Training, Awareness and Compliance

OneCall24 ensures that all staff are competent and informed in the safe, lawful, and responsible use of AI technologies.

- Staff must complete mandatory training relevant to data protection, confidentiality, and acceptable use of AI tools
- AI use guidance will be included within staff induction and reinforced through refresher training and internal communications
- Staff must understand the limitations, risks, and safeguards associated with AI use, particularly where personal or special category data is involved
- Managers are responsible for ensuring that staff understand and comply with this policy and escalate concerns appropriately
- Enhanced or role-specific training will be provided where AI use presents higher risks to individuals or organisational compliance

5. Definitions

- AI (Artificial Intelligence): Technologies that complete tasks normally requiring human intelligence, using algorithms or models.
- Data Controller: The organisation that decides how and why personal data is processed.
- Data Protection Act 2018: UK law that works alongside UK GDPR to set rules for handling personal data.

- DPO (Data Protection Officer): Internal member of staff responsible for ensuring that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with applicable data protection rules
- ICO (Information Commissioner's Office): The UK's independent authority for data protection.
- Personal Data: Any information that identifies, or could identify, a living person.
- Processing: Any action involving personal data (collecting, storing, using, sharing, etc.).
- Special Categories of Data: Sensitive information such as health, ethnicity, religion, sexual orientation, and other protected characteristics.
- UK GDPR: The retained version of the EU GDPR applicable in UK law.

6. Information for Service Users

People using our services should know that:

- We protect personal data through careful checks before using AI tools
- We only use AI in ways that comply with data-protection law
- We maintain high standards of confidentiality and security
- We remain responsible for all decisions and actions taken

7. AI-Related Incidents, Data Breaches and Reporting

OneCall24 maintains a zero-tolerance approach to unreported data protection incidents and inappropriate AI use.

Any actual, suspected, or potential data breach or misuse of AI must be reported to the Data Protection Officer (DPO) immediately.

This includes (but is not limited to):

- Entry of personal or special category data into unapproved or external AI systems
- Inappropriate reliance on AI outputs affecting care, safety, or decision-making
- Accidental disclosure, loss, or unauthorised access to personal data
- Any concern that AI use may compromise confidentiality, accuracy, fairness, or security

Incident Reporting Procedure:

- The incident must be reported immediately to the organisation's Data Protection Officer (DPO) at gdpr@onecall24.co.uk
- Staff must not attempt to investigate, resolve, or conceal the issue independently
- All relevant details must be provided, including what occurred, the data involved, and any immediate actions taken

Prompt reporting enables the organisation to:

- Assess and mitigate risks to service users and staff
- Meet statutory reporting obligations to the ICO within required timeframes
- Comply with CQC expectations around openness, governance, and safeguarding
- Prevent recurrence through corrective and preventive actions

Failure to report an incident promptly may place individuals at risk and may be treated as a serious breach of organisational policy.

8. Summary

- AI is a useful support tool, and staff are encouraged to use it safely
- Client/End User privacy and confidentiality come first
- AI supports but does not replace human judgment
- All AI-produced content must be checked for accuracy
- Seek guidance if unsure about how to use AI safely and responsibly

9. Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.