AI Policy

1. Introduction

HWW promotes the use of AI to support productivity and streamline document creation, data analysis, and communication. Users must however be aware of its limitations and the importance of human oversight, especially when dealing with sensitive information.

a) Artificial Intelligence (AI) is several different technologies working together to enable machines to sense, comprehend, act, and learn with human-like levels of intelligence.
b) AI tools are transforming the way we work. They have the potential to automate tasks, improve efficiency, increase public engagement / reach and provide valuable data-driven insights.
c) However, the use of AI tools also presents new challenges in terms of information security and data protection.
d) This policy provides practical advice on how to be safe and secure when using AI tools and establishes best practice for the responsible and ethical use of AI within the Company.

2. Scope

This policy applies to all directors, employees and volunteers of Healthwatch Worcestershire (HWW) and covers the use of all AI tools including the evaluation of security risks and the protection of confidential data. It for the safe use of AI Tools.

3. Governance and Oversight

a) Overall accountability for this policy sits with the AI lead (CB).
b) All proposed uses of AI must be assessed for risk and approved in line with this policy before adoption (including the specific tool(s) to be used).
c) AI-related risks, near-misses and incidents will be recorded and reported, please see the Escalation route d) below, to senior management as appropriate. Staff will be encouraged to report near misses for discussion / learning purposes. This discussion point will be included as fixed agenda items for both CBMs and Team meetings.
d) Escalation route:
   - stop the activity where safe to do so,
   - notify the DPO / AI lead immediately,
   - where personal data may be affected notify the DPO / report a potential breach without delay,
   - where there is potential safeguarding risk, escalate to: Children – Debbie Lamont / Adults – Julia Neal the same working day.
   - where there is significant reputational risk, escalate to the DPO (DB), or either of the Chief Officers (VW/PH) the same working day.

4. Policy Statement

a) AI must be used in compliance with all applicable legislation, regulations and organisational policies.
b) AI generated communication and documents must reflect the highs standards expected at HWW.
c) Use of AI must be in a manner that is responsible and ethical, avoiding any actions that could harm others, violate privacy, or facilitate malicious activities. Use of AI should promote fairness and avoid bias to prevent discrimination and promote equal treatment and be in such a way as to contribute positively to our goals and values.

d) Users must only use AI tools that have been approved by HWW. Approval will be sought before a tool is used and will include consideration of: the tool's security features, terms of service, privacy policy, data storage/processing locations, use of prompts/inputs for training, supplier reputation, and any third-party services or plug-ins. Where required, a DPIA and/or EIA will be completed before use.
e) Human oversight must be maintained at all times. AI outputs must not be used as the sole basis for decision-making, particularly where they may impact public information, service recommendations, or stakeholder engagement. A suitably informed person must review, sense-check and (where necessary) amend AI outputs before use or publication.
f) Only users authorised by HWW and who have received the necessary training are permitted to use company provided AI tools.
g) Employees remain responsible for the outcomes generated by AI systems and should be prepared to explain and justify how AI was used, what checks were completed, and why the final content/decision is appropriate.
h) These tools may only be used for work-related purposes and use is subject to strict adherence to these guidelines. Failure to follow these guidelines (intentional or unintentional) may result in disciplinary action.

5. Transparency

Users must be transparent about the use of AI in their work, ensuring that stakeholders are aware of the technology's involvement in our work. HWW will be open about its use of AI, particularly where outputs contribute to published reports or other public-facing content.

Below are two proposed disclosures, to be used as appropriate:

- Disclosure: the following content was generated entirely by an Artificial Intelligence (AI) based system resulting from specific requests. The AI generated content has been reviewed for accuracy and revised / edited where necessary.
- Disclosure: the following content was generated with the assistance of an Artificial Intelligence (AI) based system to augment other work. The AI generated content has been reviewed for accuracy and revised / edited where necessary.

6. Confidentiality and Data Protection

a. Employees must adhere to HWW's relevant data privacy and security policies when using AI systems.
b. Employees must maintain familiarity with relevant legislation, such as the UK GDPR and the Data Protection Act 2018. (Access to training should be discussed with the line manager if required).
c. Confidential (anything that is not in the public domain) and personal / identifiable information **must not** be entered into any open-source applications.
d. If a user is unsure whether specific information is appropriate for use with AI tools they should refer to their line manager / DPO for guidance before submitting the information.
e. Risk relating to data protection and use of AI tools will be assessed and managed proportionately. This includes (where relevant): Project Plans, Data Protection Impact Assessments (DPIAs), Equality Impact Assessments (EIAs), information security checks, and documented mitigations. Risks should be considered across categories such as: data protection/privacy, information security, accuracy and misinformation, bias and equality impacts, safeguarding/harms, legal/compliance, and reputational risk.
f. Any actual or suspected AI-related incident must be reported promptly via the appropriate route. This includes (but is not limited to): potential data breaches involving AI tools, misleading or inaccurate outputs that have been published, or outputs that indicate bias, discrimination, or harm. See 3. c) and d) above.

7. Equality, Bias and Fairness

Users must actively work to identify and mitigate biases in AI systems. In the context of health and care, particular care is required to avoid reinforcing health inequalities or unfairly impacting people with protected characteristics under the Equality Act 2010 (including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation). Outputs must be reviewed for bias, stereotyping, exclusionary language, and potential harm.

9. Copyright

Users must adhere to copyright laws when utilising AI.

10. Best practice

a) AI tools are not stand-alone solutions but are part of a wider set of resources to assist us in our operations. They should be used to supplement, not replace, traditional methods of problem-solving and decision-making.
b) The quality of the output from AI is dictated by the quality of the input. Taking time and dedicating resources to this area will result in better outputs.
c) Collaboration is encouraged to gain different perspectives, double-check the AI tool's outputs, and reduce the risk of errors.
d) Users should ensure that the personal data included in each use is accurate, adequate, relevant and limited (to the minimum amount required to fulfil the purpose).
e) Users should appropriately validate the output of AI tools. This could involve verifying the information with other reliable sources, performing rigorous testing if feasible, or consulting others when necessary.
f) Using AI tools as a supplement ensures that we retain human judgement and oversight in our processes, thereby maximising the value of these tools while minimising the associated risks.
g) Where AI is used to support recommendations or conclusions, the rationale for the final position should be recorded (including key sources/assumptions checked) so that the decision remains explainable and auditable.
h) Users of AI are responsible for reviewing output and are accountable for ensuring the accuracy of AI generated output before use/release. If a user has any doubt about the accuracy of information generated by AI, they must not publish the output.

11. Training and Education

a) HWW will provide initial training on AI policy, use and awareness with particular attention to data protection and GDPR compliance.
b) Users must undertake training specific to each tool / application prior to their use.
c) Users should also stay informed about advances in AI technology and all associated risks.

12. Alignment with External Standards and Guidance

All HWW AI activity must align and comply with

- Information Commissioner's Office (ICO) AI and data protection guidance.
- NHS England AI governance principles (as applicable to our context and partnerships).
- UK Government AI framework and associated guidance for responsible AI use.

13. Retention / deletion

- Retention: Saving Copilot output into a document/email makes it part of that record's retention rules under the HWW Data Retention Policy

- Deletion and rectification: Staff should not assume deleting a Copilot chat/output deletes the underlying source data.

14. Monitoring

HWW reserves the right to monitor all interactions with AI tools for ensuring compliance with this policy, supporting audit and assurance activity, and identifying areas for improvement. Where monitoring identifies significant non-compliance or elevated risk, this will be escalated in line with the Governance and Oversight section.

Document Details & Version Control

Version	Comments /Reason for Amendments	Lead Director	Author / Editor	Date	Review by
0.1	Draft prepared	CB	PH	15/1/25	
0.2	Updated draft prepared	CB	PH	21/1/25	
0.3	Amendments to incorporate points agreed at CBM and from ICO "How to use AI and personal data…" doc.	DB	PH	19/2/25	
1.0	Approved	DB / CB	PH	19/2/25	08/25
1.1	Proposed amendments to clause 3,d)	DB / CB	PH	21/8/25	
1.2	Comprehensive amendments following guidance from JN	DB / CB	JN / PH	22/4/26	
1.3	Further changes to incorporate appropriate guidance from the Copilot DPIA	DB / CB	PH	27/4/26	
2.0	Approved at CBM 14.5.26	DB	PH	14/5/26	11/26