



Hale Community & Youth Centre

Draft Generative AI User Policy

*'Consider Environmental Impact -
Avoid Unnecessary AI Use'*

Hale Community and Youth Centre are committed to using Generative AI tools - such as those that create text, images, audio, or video - to drive innovation, improve efficiency, and enhance our services in line with our charitable objectives.

While recognising the potential benefits, we are also mindful of the associated risks, such as bias and data security. This policy outlines the goals, use, and guidelines around using Generative AI tools in a safe and ethical manner. It should be read in compliance with any future handbook and as an extension to our company values.

This policy applies to all trustees, employees, volunteers, contractors, and any other individuals acting on behalf of Hale Community and Youth Centre who use or interact with AI systems or data used for AI development in their work for the charity.

1. ETHICAL USE OF AI

We support the use of Generative AI to enhance, but not replace, human expertise. All use must align with our values of inclusivity, transparency, and accountability.

1) Permitted Uses. Generative AI may be used to:

- Improve administrative efficiency
- Support creative projects and communications
- Enhance service delivery and engagement
- Generate ideas and draft content for review.
- Improving fundraising efforts.

2) Prohibited Uses. Generative AI must not be used to:

- Create misleading or deceptive content.
- Replace safeguarding or professional judgment.
- Circumvent data protection or privacy obligations.
- Generate discriminatory, biased, or harmful outputs.

2. APPROVED AI TOOLS

ChatGPT, Microsoft Copilot, Google Gemini and Grammarly are the tools accepted for use at Hale Community and Youth Centre with adherence to the guidelines above. Please use the official login and account when provided.

3. USING GENERATIVE AI

All users are responsible for ensuring ethical and lawful use of AI tools. Concerns or breaches must be reported to the designated Safeguarding Lead. A review will be conducted to assess impact and decide corrective actions.

4. LEGAL COMPLIANCE

AI generated content may inadvertently include copyrighted material. Users must verify sources to ensure originality and compliance with intellectual property laws.

5. BIAS MITIGATION

As we are accountable for the use of AI within our organisation, we will regularly review and evaluate the impact of any AI systems and take steps to address any unintended consequences.

7. REPORTING CONCERNS

Any concerns about the use of AI within Hale Community and Youth Centre, including potential breaches of this policy or ethical concerns, should be reported at once to the designated Safeguarding Lead

8. POLICY REVIEW

This policy will be reviewed and updated regularly, at least annually, to reflect changes in AI technology, best practices, and legal requirements.

IMPORTANT CONSIDERATIONS FOR UK CHARITIES:	
1)	Fundraising Regulator: Be mindful of the Fundraising Regulator's guidance on the use of data and technology in fundraising.
2)	Charity Commission: Consider the Charity Commission's guidance on data protection and cybersecurity.
3)	ICO (Information Commissioner's Office): The ICO is the UK's independent body for data protection and freedom of information. Stay up to date with their guidance on AI and data protection.
4)	Equality Act 2010: Ensure that AI systems do not discriminate against individuals based on protected characteristics under the Equality Act 2010.
5)	Human Rights Act 1998: Be aware of the potential impact of AI on human rights, such as the right to privacy and freedom of expression.
6)	Safeguarding: If AI is used in areas related to safeguarding, ensure robust safeguards are in place to protect vulnerable individuals.
7)	Explainability: Focus on making AI systems as explainable as possible, especially when they are used to make decisions that affect individuals. This helps build trust and accountability.
8)	Impact Assessments: Conduct regular impact assessments of AI systems to find and mitigate potential risks. Consider using a Data Protection Impact Assessment (DPIA) where necessary.
9)	Algorithmic Transparency: Where possible, strive for algorithmic transparency, meaning that the logic and processes behind AI systems are understandable.