

Policy Group: Information Governance & IT		Policy no: 3.4.11
Review Date: Jul 25	Last review: New policy	Next review due: July 2030
Approved by: SMT and Comms Working Group		Approval date: 20/08/2025

3.4.11 Artificial Intelligence Policy

Contents:

1. Purpose of Policy
2. Usage Principles
3. Risk Mitigation
4. Guidance for KCSC Staff and Volunteers
5. Compliance and Data Protection

1. Purpose of policy

At KCSC, we recognise the potential of Artificial Intelligence (AI) to enhance our services, improve efficiency, and support our mission and strategic objectives. This policy outlines how AI is used within our organisation to ensure it aligns with our values, remains ethical, and benefits our staff, volunteers, and the communities we serve.

This policy applies to all staff, trustees, volunteers, and partners using AI tools as part of their roles. It covers AI-driven services such as research assistance, automated recommendations, and any other AI applications we adopt. It sets out clear principles for responsible AI use, ensuring accuracy, transparency, data protection, and human oversight.

By adhering to this policy, we ensure AI remains a tool that supports—not replaces—human expertise while upholding our commitment to fairness, privacy, and inclusivity.

2. Usage Principles

Our AI-driven uses are governed by clear principles. These principles ensure the AI benefits all users and operates ethically. They are informed by sector best practices (e.g. The National Lottery Community Fund's AI principles):

- **Human-Centric and Empowering:** AI enhances human expertise; it does not replace it. For example, our AI research tool gathers information swiftly, allowing staff to focus on personalised advice.
- **Human Oversight:** Significant AI-driven processes involve human review to ensure outputs are appropriate and mission-aligned.
- **Transparency and Accountability:** We inform users when AI-generated content is provided. We take responsibility for AI outputs and address any issues that arise.

- **Inclusivity and Accessibility:** Our use of AI services is designed to be unbiased and accessible, catering to users regardless of digital literacy, background, or ability. We offer alternative support methods, like phone or email assistance, to ensure inclusivity.
- **Privacy and Data Security:** We protect user privacy by minimising data collection and ensuring no personal data is used without consent. Our AI systems comply with UK data protection laws, including GDPR. Our website states where information is stored, e.g. chat sessions on the user's device and temporarily on the OpenAI servers.
- **Ethical Use and Fairness:** AI applications align with our charity's ethical values. We conduct small-scale trials before full deployment and assess the environmental and societal impacts of AI use.
- **Continuous Improvement:** We monitor AI usage and outcomes, regularly updating systems and policies to adapt to best practices and regulations. User feedback is actively sought to evolve our approach.

3. Risk Mitigation

We have assessed potential risks that AI could pose in our services and developed strategies to mitigate each risk. The following register identifies key operational, ethical, reputational, and compliance risks specific to our charity's AI use, along with how we address them:

- **Misinformation:** AI tools may produce incorrect information. **Mitigation:** Use up-to-date content, undertake testing and verification of AI content; staff review AI-generated outputs before releasing a system.
- **Bias and Fairness:** AI systems can inadvertently carry biases. **Mitigation:** Use diverse training data (where applicable), conduct bias review, and provide mechanisms for users to report biased AI responses. Ensure human review and validation processes are in place.
- **Data Privacy and Security:** AI applications could pose data privacy risks. **Mitigation:** Conduct Data Protection Impact Assessments, exclude personal data from AI training, secure AI systems per IT security policies and minimise data collection. We advise users not to enter personal or confidential information.
- **Reputational Damage:** AI errors could harm our or our user's charity reputation. **Mitigation:** Ensure human accountability, set usage boundaries, and have an incident response plan for AI errors. Advise users accordingly.
- **Dependency on AI:** Over-reliance on AI could weaken human skills. **Mitigation:** Treat AI as a support tool, provide staff training, and have fall-back procedures for AI system failures. Advise users of the same.
- **Accessibility and Digital Exclusion:** Some users may struggle with AI tools, and others may be dramatically enabled. **Mitigation:** Design AI to be user-friendly, adhere to accessibility standards, and offer alternative support methods, and personal coaching.

4. Guidance for KCSC staff and volunteers

Our internal AI policy guides staff and volunteers on responsible AI use. Staff are required to be familiar with our AI usage principles as outlined in this policy and ensure they are followed in practice. Staff are made aware that:

- AI should assist, not replace, human decision-making and they remain responsible for verifying AI-generated content before using it in decision-making, reports, or

communications. Critical decisions (e.g., legal, financial, or HR-related) require human review.

- Staff must verify AI outputs against reliable sources before acting on them. AI generated information should not be assumed to be correct without validation. Employees should cross-check facts, figures, and legal/statutory guidance where appropriate, AI should be used as a tool to support accomplishing a task and staff are encouraged to utilise their own critical thinking, independent judgment, knowledge and collaboration.
- Sensitive, confidential, or personal information should not be inputted into AI tools unless they are configured to maintain privacy and data protection regulations must be followed at all times.

Project specific guidance around the use of AI will be added to this policy as Appendices as appropriate.

5. Compliance and Data Protection

KCSC is committed to protecting the privacy and security of our users, staff, and stakeholders. Our use of AI is guided by strict data protection principles to ensure compliance with UK laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

- **Minimal Data Collection:** We only collect and process the data necessary to provide services. Personal or sensitive data is never entered into AI tools unless explicitly required.
- **User Privacy:** AI-generated interactions, such as chatbot conversations, will be utilised in a way to protect privacy.
- **Transparency:** We clearly inform users when AI is being used and explain how it interacts with their data.
- **Security Measures:** We take appropriate technical and organisational measures to safeguard data.
- **Third-Party AI Tools:** If external AI services are used, we ensure they meet data protection standards and do not compromise user privacy.