

ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY

I. PURPOSE

The purpose of this policy is to define guidelines for the appropriate handling of Artificial Intelligence (AI) tools at Skills & Volunteering Cymru (SVC). It focuses on mitigating the risks associated with AI usage, ensuring that any use of AI (including generative AI programs, E.G. Microsoft Copilot), is conducted securely and responsibly. This policy does not promote the use of AI but provides clear directives for its management if utilised.

Microsoft Copilot, accessed through an SVC work account, is the only AI tool that may be used for SVC work. No other AI tool is approved, for any task, on any device.

This policy sets out how Copilot may be used safely and responsibly at Skills & Volunteering Cymru (SVC). It does not require anyone to use AI. Its aim is to manage the risks if Copilot is used:

- **Data Storage and Leakage:** AI tools often rely on cloud-based systems, raising concerns about where sensitive information is stored. Misuse or improper configuration can lead to data breaches or leaks, compromising confidentiality.

- **Confidentiality Risks:** Generative AI tools may unintentionally process or retain sensitive data shared during interactions, posing risks to privacy and organisational trust.
- **Economic Risks:** Over-reliance on AI could inadvertently devalue human skills or lead to resource misallocation if tools are used without careful planning or oversight.
- **Social Risks:** AI outputs may unintentionally reinforce biases, misinformation, or exclusion, impacting SVC's commitment to inclusivity and fairness.

This policy ensures AI use aligns with SVC's values by prioritising secure handling, ethical practices, and thoughtful integration. Restricting SVC to one tool, set up and controlled through our Microsoft account, lets us apply consistent security, training and oversight.

II. SCOPE & DEFINITIONS

This policy applies to all staff, volunteers and trustees at Skills & Volunteering Cymru (SVC) and covers the use of all AI tools provided by the charity.

Term	**Meaning in this policy**
AI tool	Any software that generates or analyses text, images, audio, video or data using artificial intelligence. This includes chatbots, writing assistants, AI features inside other apps, browser extensions, and meeting recorders or note-takers.
Copilot	Microsoft Copilot (Microsoft 365 Copilot Chat, and Microsoft 365 Copilot where SVC has licensed it), used while signed in with a SVC work account.
Personal data	Any information that identifies a living person, such as names, email addresses, phone numbers, addresses, dates of birth, photos or case notes.
Special category data	Personal data about health, disability, ethnicity, religion, sexual orientation, criminal records or similar sensitive matters.
Confidential information	Contracts, funding bids, partnership details, finances, HR matters, and anything not intended for the public.

Authorised user	A user who has completed SVC's Copilot training and permitted by the SVC Manager.

III. POLICY

1. Authorised Use

Only staff, volunteers and trustees authorised by Skills & Volunteering Cymru and who have received the necessary training are permitted to use AI tools. Authorised AI users will be notified of their updated permissions by the SVC Manager once the appropriate training has been conducted. Requests for this specific training should be made directly to the SVC Manager. This authorisation process is necessary to ensure that users understand the capabilities and limitations of these tools and use them effectively and responsibly.

Unauthorised use includes usage by non-authorised personnel (those that have not undergone the necessary training and received permissions from the SVC Manager), actions beyond one's work scope (E.G. generating official reports or analysing data), or use inconsistent with this policy. Report any suspected misuse (I.E. using AI tools without authorisation, performing tasks outside designated responsibilities, or violating data security and policy guidelines) to the SVC Manager immediately. Unauthorised usage may result in disciplinary action, up to and including termination of employment and/or volunteering roles.

2. Data Security and Confidentiality

Preservation of company data security, intellectual property, and confidentiality is paramount in all activities, including the use of AI tools. As these tools learn and generate content based on the input data, it is crucial that users avoid inputting or sharing sensitive, confidential or restricted information, such as volunteer data (including, but not limited to, personal information such as names and contact details), confidential contracts, details about partnerships, projects, work statements, or any other proprietary information.

Furthermore, users must respect the legal and ethical boundaries concerning data privacy. If an individual is unsure whether specific information is appropriate to use with the AI tool, they should consult the SVC Manager. Violations of data security and confidentiality guidelines will be treated as a serious violation.

3. Use of AI Tools as Supplemental Resources

AI tools are not stand-alone solutions but can be part of a wider set of resources to assist staff, volunteers and trustees in their roles. They should be used to supplement, not replace, traditional methods of problem-solving and decision-making.

The output of AI tools should always be supplemented with business logic. Business logic involves utilising human judgement and expertise when applying the organisation's principles and strategic understanding to make informed decisions. For instance, if the authorised AI tool generates a suggestion or plan, users should critically evaluate the suggestion using their understanding of the charity’s values, aims and strategic plan.

Furthermore, collaboration with colleagues is encouraged to gain different perspectives, double-check the AI tool's outputs, and reduce the risk of errors. Additionally, staff, volunteers and trustees should appropriately validate the output of AI tools. This could involve cross-verifying the information with other reliable sources.

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.

4. Risk Assessments for Artificial Intelligence Usage

In the course of using AI tools, staff, volunteers and trustees should always be aware of the inherent risks these technologies pose. These may include potential inaccuracies or misinterpretations in AI-generated content due to lack of context, legal ambiguities concerning content ownership, and possible breaches of data privacy. As such, a critical attitude towards AI outputs is required at all times.

Authorised AI users should conduct risk assessments when using AI at any time. All assessments should be documented in accordance with SVC Policy when inputting any data into an AI tool.

5. Use of Third-Party AI Platforms

Staff, volunteers and trustees should exercise caution when using third-party AI platforms due to the potential for security vulnerabilities and data breaches. Before using any third-party AI tool, staff, volunteers and trustees are required to verify the security of the platform. This can be done by checking for appropriate security certifications, reviewing the vendor's data handling and privacy policies, and consulting with the SVC Manager.

Moreover, data shared with third-party platforms must comply with the guidelines outlined in Section III(2) - Data Security and Confidentiality. In situations where individuals are unsure about the use of a third-party platform, they should seek guidance from their supervisors or the SVC Manager.

6. Use in Communications

AI tools should not be used to create content for internal or external communication. While AI tools may be utilised by authorised users to support content editing, they should not be used to generate the main body or messaging of our communications. Any output from AI tools that is used should always be reviewed carefully. Any misuse of AI tools for communication, including any language or behaviour that violates the charity's policies, will be treated as a serious violation.

The below is a non-exhaustive set of examples of what would be considered misuse. Individuals should always consult the SVC Manager if they are uncertain about their use-case.

Internal Communication:

- Using AI to draft or respond to emails, direct messages, or internal memos without approval.
- Generating automated messages to staff that could include inaccurate or inappropriate information.

External Communication:

- Employing AI to draft responses to inquiries from beneficiaries, partners, or stakeholders, particularly when sensitive or confidential information is involved.

- Using generative AI to create social media posts, newsletters, or promotional materials without prior review for accuracy and alignment with SVC's tone and mission.

Client and Beneficiary Interaction:

- Automating responses to beneficiaries using AI in a way that lacks personalisation or could misinterpret their needs.
- Relying on AI to handle sensitive discussions about services, support, or accommodations.

Policy or Official Statements:

- Using AI to draft official policies, public statements, or reports without proper oversight, risking inaccuracies or misrepresentation.

Training and Guidance Materials:

- Using AI-generated content for volunteer training, guidance documents, or role descriptions without verification, which could lead to incomplete or misleading information.

7. Use in Research and Development

AI tools, including but not limited to language models and machine learning algorithms, can serve as valuable assets in streamlining the research and development processes within Skills & Volunteering Cymru's work. They can expedite data analysis, facilitate trend identification, accelerate prototyping, and augment creative brainstorming.

However, when employing AI tools for Research & Development purposes, all usage must strictly align with our intellectual property and data security policies. Intellectual property generated through the use of AI tools remains the property of Skills & Volunteering Cymru.

Additionally, any data used in conjunction with AI tools for Research & Development, whether it's proprietary, volunteer-data, or otherwise sensitive data, must be handled according to our data security policies. This includes ensuring appropriate anonymisation or pseudonymisation of sensitive data, and proper access controls. Any data used with AI tools must follow our data security rules, protecting sensitive information by anonymizing it and controlling access.

8. Non-Personal Use

Any AI tools provided by Skills & Volunteering Cymru are for business use only and should not be used for personal activities. This policy is in place to ensure the maintenance of a professional environment, the preservation of the charity's resources, and to prevent potential legal and security risks.

Personal use of these tools could potentially involve sharing of inappropriate or sensitive content, misuse of company time and resources, and potential breach of data privacy regulations. Therefore, staff, volunteers and trustees are expected to refrain from using AI tools, provided by the charity, for non-work-related tasks.

In instances where the line between professional and personal use might be blurred (e.g., professional development), individuals are encouraged to seek approval from their supervisor.

9. Monitoring

Skills & Volunteering Cymru reserves the right to monitor all interactions with AI tools to ensure compliance with this policy. Monitoring may involve a combination of automated and manual checks, such as reviewing usage logs and tracking specific activities where AI is used. Any data collected will be used strictly for policy compliance purposes.

10. Violations

Breaches of this policy may lead to disciplinary action, including potential termination of employment.

IV. POLICY COMPLIANCE

The SVC Manager is responsible for regularly monitoring compliance with this policy. Any policy breaches will be promptly investigated and appropriate actions will be taken to address and resolve the issue.

V. REVIEW AND REVISION

This policy will be reviewed and updated periodically to accommodate changes in technology, business needs, or legal requirements.