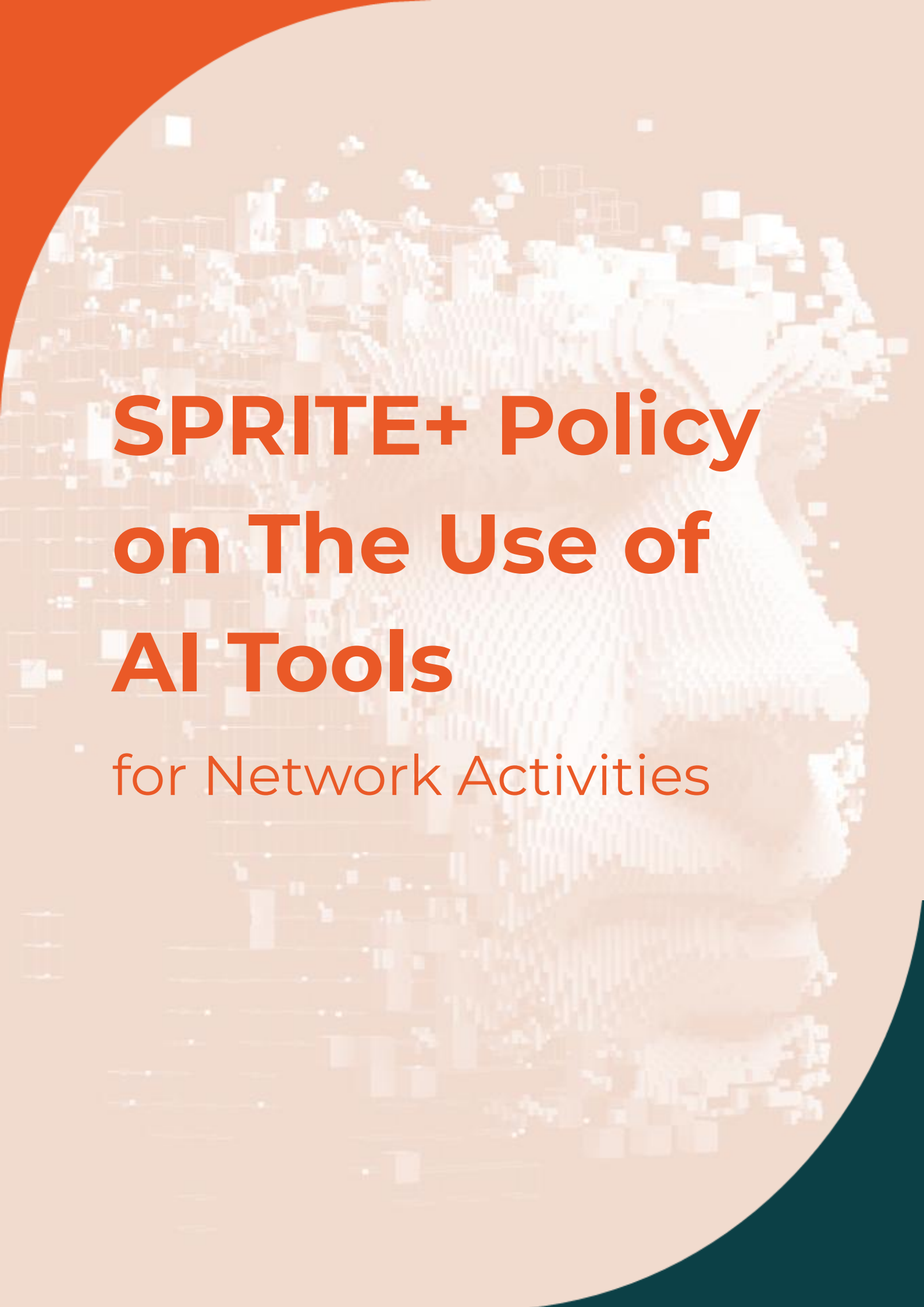




SPRITE+ Policy on The Use of AI Tools

for Network Activities

Table of Contents

1. Purpose and scope	3
2. Definitions.....	3
3. Use of Microsoft 365 Copilot within SPRITE+.....	3
3.1 Core Use Cases	3
3.2 Data Protection and Training of Models (Microsoft 365 Copilot).....	4
4. Use of Other AI Tools (ChatGPT, Claude, and Similar)	5
4.1 Public / Consumer AI Services	5
4.2 Model Training and Data Retention (Non-Microsoft Tools).....	5
5. Use of AI with Anonymised Members' Data	5
5.1 Permitted use	5
5.2 Prohibited use	6
6. Use of AI in Airtable	6
7. Security, Confidentiality, and Access Control	6
8. The University of Manchester Guidelines for Staff Using or Developing AI.....	7



SPRITE+ Project Team, Humanities Bridgeford Street, University of Manchester, Oxford Road M13 9P



1. Purpose and scope

This policy sets out how AI tools (including Microsoft Copilot, ChatGPT, Claude, and similar systems) may be used for SPRITE+ network activities, with a particular focus on:

- **Microsoft 365 Copilot** integrated into Word, Excel, PowerPoint, Outlook, Teams and other Microsoft 365 apps.
- **Use of AI for summarising and analysing documents and anonymised member data** (e.g. grant applications, reports, surveys).

2. Definitions

- **AI tools:** Generative or conversational AI systems such as Microsoft Copilot, Microsoft 365 Copilot, ChatGPT, Claude, and similar services.
- **Microsoft 365 Copilot:** The AI functionality embedded in Microsoft 365 apps that can read, summarise, and answer questions about content stored in Microsoft 365 (e.g. OneDrive, SharePoint, Exchange) according to existing permissions.
- **Personal data:** Any information relating to an identified or identifiable natural person, as defined under UK GDPR.
- **Anonymised data:** Data that has been processed so that individuals are no longer identifiable, and re-identification is not reasonably likely.
- **Pseudonymised data:** Data where identifiers are replaced with codes, but re-identification remains possible by using additional information.

3. Use of Microsoft 365 Copilot within SPRITE+

3.1 Core Use Cases

Due to [recent agreements between Microsoft and the University of Manchester](#), colleagues have been encouraged to use Copilot across Microsoft 365 apps as well as the chat function, including:

- **Document understanding and Q&A:**
 - Asking Copilot to read a document (e.g. Word, Excel, PowerPoint, PDF stored in OneDrive/SharePoint) and:
 - Generate concise or detailed summaries.
 - Extract key points, risks, actions, or decisions.
 - Answer questions about the document's content.



SPRITE+ Project Team, Humanities Bridgeford Street, University of Manchester, Oxford Road M13 9P

- **Email and communication support:**
 - Drafting, summarising, or rephrasing emails and messages, with human review before sending.
- **Data and reporting support:**
 - Summarising tables, extracting trends, and drafting narrative text for reports or board papers, based on data stored in Microsoft 365.

All such use remains within the University of Manchester Microsoft 365 tenant and respects existing permissions and access controls.

3.2 Data Protection and Training of Models (Microsoft 365 Copilot)

For Microsoft 365 Copilot in the organisational environment:

- Prompts, responses, and data accessed through Microsoft Graph (emails, documents, chats, etc.) are not used to train the foundation large language models that power Microsoft 365 Copilot¹.
- Microsoft states that “your data stays your data” and that files or communications with Copilot are not used to train models or shared with other customers².

This means that, within the University of Manchester Microsoft 365 environment, Copilot is not an open-source or public training system: organisational content is processed to provide responses but is not fed back into the underlying foundation models.

References:

- The University of Manchester – [*AI Partnership Between the University of Manchester and Microsoft Announced*](#)
- ¹Microsoft Learn – [*Data, Privacy, and Security for Microsoft 365 Copilot*](#)
- ²Microsoft Learn – [*Microsoft 365 Copilot data and compliance readiness*](#)

SPRITE+ will continue to treat Copilot as a cloud service subject to Microsoft’s privacy and security commitments and the University of Manchester’s own data protection obligations.



SPRITE+ Project Team, Humanities Bridgeford Street, University of Manchester, Oxford Road M13 9P



4. Use of Other AI Tools (ChatGPT, Claude, and Similar)

4.1 Public / Consumer AI Services

Public or consumer versions of AI tools (e.g. ChatGPT on the open web, non-enterprise Claude, non-managed Copilot experiences) will be treated as external services. In these tools, SPRITE+ Team Members:

- **Will not input:**
 - Personal data about identifiable individuals (members, applicants, staff, partners).
 - Confidential, commercially sensitive, or security-sensitive information.
 - Non-public documents or data that SPRITE+ is obliged to protect.
- **Permitted inputs:**
 - Fully anonymised or synthetic data.
 - Publicly available information.
 - High-level, non-sensitive descriptions of tasks or processes.

4.2 Model Training and Data Retention (Non-Microsoft Tools)

Different AI providers have different policies on whether user data is used to train their models. It is not and should not be assumed that external tools behave like Microsoft 365 Copilot. Before using any non-Microsoft AI tool for SPRITE+ work, users must restrict use to anonymised or synthetic data.

5. Use of AI with Anonymised Members' Data

5.1 Permitted use

AI tools (including Copilot, ChatGPT, Claude, or similar) may be used to generate summaries, analyses, or draft text based on anonymised members' data, for example:

- Grant or funding applications (e.g. summarising anonymised application content, extracting themes, drafting templates).
- Survey responses where all direct and indirect identifiers have been removed.
- Event feedback where responses are aggregated and anonymised.



SPRITE+ Project Team, Humanities Bridgeford Street, University of Manchester, Oxford Road M13 9P



In these cases:

- Data should be anonymised before being entered into any AI tool.
- Where pseudonymisation is used (e.g. coded IDs), additional care must be taken to ensure that no re-identification is possible by the AI tool or its provider.

5.2 Prohibited use

- Uploading raw, identifiable member data (e.g. names, email addresses, CVs, detailed biographies, sensitive categories) into public AI tools.
- Using AI outputs as the sole basis for decisions that significantly affect individuals.

Human judgement must always remain central, and AI outputs must be treated as advisory.

6. Use of AI in Airtable

AI features within Airtable will only be used in ways that are consistent with our privacy policy and in particular, adhere to GDPR's data-minimisation principle. Airtable will be used to store membership records and event-participation details, and any AI-driven processing of this data will remain strictly within SPRITE+'s Delivery Team workflow in a manner that remains consistent with our Privacy Policy. AI may be used to support operational tasks such as structured data cleaning, validation, or summarisation, but will never be applied to infer sensitive attributes, profile individuals, or generate decisions that affect member rights or access. AI may also be used to generate summaries of project data for internal administrative purposes.

7. Security, Confidentiality, and Access Control

- Microsoft 365 Copilot operates within the existing Microsoft 365 security and compliance framework; it respects the same permissions and access controls as SharePoint, OneDrive, Exchange, and Teams.
- The SPRITE+ Team:
 - Ensures documents are stored in appropriate locations with correct permissions before using Copilot to summarise or query them.
 - Avoids using Copilot to surface or share content with individuals who do not have permission to access the underlying files.
- Sensitive or restricted documents must be protected using appropriate Microsoft 365 controls (e.g. sensitivity labels, access restrictions) before being used with Copilot.



SPRITE+ Project Team, Humanities Bridgeford Street, University of Manchester, Oxford Road M13 9P

8. The University of Manchester Guidelines for Staff Using or Developing AI

The [document](#) outlines the University of Manchester's principles and policies for the responsible use and development of AI by staff and students. It emphasises transparency, accountability, competence, and ethical use across teaching, learning, research, and operational activities. Alongside this, it addresses risks such as bias, data privacy, and academic integrity, and providing detailed guidance on AI tool use, referencing, and access.

As SPRITE+ is based at the University of Manchester, SPRITE+ practices should comply with these guidelines.



SPRITE+ Project Team, Humanities Bridgeford Street, University of Manchester, Oxford Road M13 9P

