



Artificial Intelligence Policy

Effective from: 02/07/2026

Author: Practice, Governance & Training Sub-Committee

Review date: 02/07/2027

Version 1.0

CONTENTS

<i>POLICY FRAMEWORK AND CONTEXT</i>	3
PURPOSE	3
SCOPE	3
CONTEXT	3
KEY PRINCIPLES IN PRACTICE	3
<i>AI RISK LEVELS</i>	4
<i>PERMITTED AND PROHIBITED USES</i>	5
EXAMPLES OF PERMITTED USES	5
EXAMPLES OF PROHIBITED OR RESTRICTED USES	5
DATA PROTECTION AND INFORMATION HANDLING	6
Information Handling Guide.....	6
APPROVED TOOLS AND ACCOUNTS	6
<i>GOVERNANCE AND ACCOUNTABILITY</i>	7
IF YOU ARE UNSURE, CONCERNED OR BELIEVE YOU HAVE MISUSED AI	7
ACCURACY, QUALITY AND INTELLECTUAL PROPERTY	7
AI-ENABLED FRAUD AND MISUSE RISKS	7
TRAINING AND WELLBEING	7
ETHICAL FOUNDATIONS	8
REVIEW AND POLICY EFFECTIVENESS	8
QUESTIONS	8
POLICY CHANGE SHEET	9

POLICY FRAMEWORK AND CONTEXT

PURPOSE

To outline to all Cruse Scotland staff members, volunteers, trustees, third-party stakeholders, contractors and consultants the current procedures and protocol for working with artificial intelligence (AI).

SCOPE

This policy applies to all Cruse Scotland staff members, volunteers, trustees, third-party stakeholders, contractors and consultants. It covers all uses of AI for work undertaken on behalf of Cruse Scotland, including organisation-provided tools, third-party tools and publicly available AI systems.

This policy applies specifically to work carried out for or by Cruse Scotland and may differ from how individuals use AI in other organisations or in a personal capacity. The policy includes training materials, training feedback, research outputs, internal strategy documents and other intellectual property created or held by Cruse Scotland.

CONTEXT

Cruse Scotland recognises that artificial intelligence (AI) tools are increasingly available and may offer benefits for internal efficiency and administrative work. However, their use also raises ethical, legal and safeguarding risks, particularly given the organisation's work with people affected by bereavement.

As a national charity supporting people through bereavement, Cruse Scotland places a high value on trust, professional judgement and human care. This policy therefore takes a deliberately cautious approach to AI use, prioritising safeguarding and confidence in our services over efficiency gains.

While AI tools may be used to support internal development, training, quality improvement and service enhancement, their deployment in areas such as client support, counselling, safeguarding decision-making or the handling of client data must be subject to appropriate governance, human oversight and data protection controls.

Cruse Scotland recognises that AI technologies may evolve and that carefully governed exploration or pilot development ("sandbox" use) may at times be appropriate. Any such development must be formally approved and subject to safeguarding, data protection and ethical review before testing or implementation.

This policy outlines how AI may and may not be used and provides guidance for staff, volunteers and contractors when considering AI use in their work.

KEY PRINCIPLES IN PRACTICE

- **AI should not be used in direct client support or counselling without explicit organisational approval**, appropriate oversight, and clear human accountability.
- **AI must not process client or beneficiary data unless this use is lawful**, proportionate and compliant with UK data protection law and the organisation's safeguarding duties.

- **AI may support professional practice, training and service development**, but it does not replace professional judgement, ethical responsibility or regulatory obligations.
- **Accountability for AI-assisted work remains with the human user** and, where relevant, the organisation.
- **Where there is uncertainty about the appropriateness, legality or ethical implications of AI use, staff must pause and seek advice** before proceeding.
- **Where AI materially contributes to content or tools used in client-facing contexts, transparency must be maintained** and AI use must not be misleading or hidden.

DEFINITION OF ARTIFICIAL INTELLIGENCE

For the purposes of this policy, Cruse Scotland adopts the definition used in the Scottish Council for Voluntary Organisations (SCVO) AI Guidelines (v1.0):

Artificial Intelligence (AI) refers to digital systems that are designed to perform tasks that normally require human intelligence. This includes tools that generate text, images, audio or code, analyse data, or make predictions based on patterns in information.

This includes (but is not limited to):

- **Large language models (e.g. text-based generative AI)**

Examples: ChatGPT (OpenAI), Claude (Anthropic), Gemini (Google), Microsoft Copilot.

- **Transcription or summarisation tools**

Examples: Otter.ai, Microsoft Teams transcription, Zoom AI Companion, Fireflies.ai, Read.ai.

- **Chatbots**

Examples: Website customer-service chatbots, AI-powered FAQ bots, automated mental health support bots such as Woebot, or bespoke organisational chat interfaces built on LLMs.

- **Predictive or analytical systems**

Examples: Risk-scoring algorithms, safeguarding flagging systems, demand forecasting tools, sentiment analysis platforms, or machine learning models used to identify patterns in service usage data.

AI RISK LEVELS

Cruse Scotland recognises that not all AI use carries the same level of risk. The level of governance, oversight and approval required will depend on the context of use.

- **Low Risk**

Use of AI for generic administrative or developmental tasks involving non-sensitive information.

Examples include drafting internal documents, generating training ideas, formatting text, summarising publicly available information, or planning work.

- **Medium Risk**

Use involving internal confidential information, organisational strategy, HR matters, or external communications made on behalf of Cruse Scotland.

Such uses require managerial oversight and must comply with data protection and organisational policies. Public-facing content generated with AI must always receive appropriate human review and formal sign-off before publication.

- **High Risk**

Any use involving service users, client or beneficiary data, safeguarding matters, counselling or therapeutic content, or decisions affecting service delivery.

High-risk uses require explicit organisational approval, documented governance controls (including a DPIA where required), and clear human oversight. In the absence of such approval and safeguards, these uses must not proceed.

PERMITTED AND PROHIBITED USES

EXAMPLES OF PERMITTED USES

AI tools may be used for internal, back-office and administrative purposes, subject to appropriate safeguards and approval where required. Examples include:

- Drafting, summarising or editing internal documents and reports
- Improving clarity, grammar or structure of non-client-facing communications
- Supporting administrative tasks, planning or idea generation
- Assisting with analysis of non-personal, non-sensitive data
- Productivity support within organisation-approved tools

Staff must not input confidential, strategic, HR-related or otherwise sensitive organisational information into external AI systems unless the system has been formally approved and appropriate data protection and contractual safeguards are in place.

All AI-generated outputs must be reviewed, checked and approved by a human before use. Human users remain responsible for the accuracy, appropriateness and compliance of any material produced with AI assistance.

EXAMPLES OF PROHIBITED OR RESTRICTED USES

The following uses are not permitted unless formally approved, risk assessed and subject to appropriate governance, oversight and safeguarding controls:

- Processing, analysing or generating content using client or beneficiary data without lawful basis, data protection compliance and documented safeguards (including a DPIA where required).
- Producing or influencing live counselling, therapeutic or bereavement support content without explicit organisational approval and clear human oversight.
- Making automated decisions about service users, eligibility, risk or support pathways without meaningful human involvement and formal governance approval.
- Predicting or assessing emotional or mental states of clients in ways that could affect support decisions, unless part of an approved and risk-assessed pilot or system development process.
- Uploading personal, sensitive, confidential or strategic organisational information into unapproved external AI systems.
- Impersonation, deception or the creation of misleading or fabricated content.
- Any use that could reasonably cause harm, distress, misrepresentation or loss of trust.

The development of new AI-supported processes (e.g. triage, intake, allocation or contact management systems) must undergo formal approval, safeguarding review, data protection assessment and senior leadership sign-off before testing or implementation.

DATA PROTECTION AND INFORMATION HANDLING

All AI use must comply with **UK GDPR, the Data Protection Act 2018**, and Cruse Scotland's data protection and privacy policies.

Users are responsible for understanding whether AI functionality is enabled within the software and devices they use for work purposes. Where AI features (such as automated transcription, predictive text or cloud-based summarisation) are enabled by default, users must ensure these are configured in line with this policy or disabled where appropriate.

Information Handling Guide

Red – Never use with AI

Identifiable client or service user information; counselling notes; safeguarding concerns; health or special category data; contact details; incident reports; confidential case records.

Amber – Only with explicit CEO approval

Internal confidential strategy documents; sensitive HR matters; non-public partner or funder information.

Green – Generally permitted

Generic administrative content; templates; formatting; non-sensitive internal communications; anonymised or synthetic examples.

Users must assume that externally hosted AI tools may retain or process any material uploaded to them, including any 'identifiers' such as the use of the Cruse Scotland name and brand.

APPROVED TOOLS AND ACCOUNTS

Where available, staff and volunteers (where applicable) must use organisation-provided AI tools and accounts. Personal AI accounts must not be used for work-related material. The

introduction of any new AI tool requires approval by the CEO (or delegated authority) following consideration of data protection, safeguarding, contractual, ethical and reputational risks.

GOVERNANCE AND ACCOUNTABILITY

Overall responsibility for the governance, approval and oversight of AI use rests with the Chief Executive Officer (CEO). The CEO is responsible for approving new AI tools, significant changes to AI use, and any AI use that may introduce ethical, safeguarding or data protection risks. The CEO may delegate specific responsibilities while retaining overall accountability.

Day-to-day responsibility sits with individual users and line managers. Where AI use raises safeguarding concerns, these will be managed in line with Cruse Scotland's safeguarding policies and procedures.

Cruse Scotland recognises that AI tools are widely available and that staff and volunteers may have questions. Seeking advice or clarification about AI use is encouraged and will not be treated as misuse.

However, any suspected misuse of AI, unintended data disclosure, or use outside this policy must be reported promptly and will be managed in line with existing data protection and safeguarding incident procedures.

IF YOU ARE UNSURE, CONCERNED OR BELIEVE YOU HAVE MISUSED AI

If you are unsure or concerned about AI use:

1. Stop using the AI tool for the task in question
2. Do not attempt to resolve the issue alone
3. Raise the concern with your Line Manager
4. Where safeguarding or confidentiality may be affected, existing safeguarding procedures apply

ACCURACY, QUALITY AND INTELLECTUAL PROPERTY

AI outputs may be inaccurate, incomplete or misleading. AI will often adjust its outputs to align them with the engagement of the user (known as the obsequiousness problem) this can enhance existing mistakes and biases. Users must verify factual claims, ensure appropriate sourcing, and take responsibility for final content. AI must not be used to generate or reproduce content that infringes copyright, intellectual property or confidentiality obligations.

AI-ENABLED FRAUD AND MISUSE RISKS

AI tools may be used maliciously to enable phishing, impersonation or fraud. Unusual or unexpected requests, particularly those involving payments or changes to financial details, should be treated as suspicious and handled in line with existing finance and security procedures.

TRAINING AND WELLBEING

Staff and volunteers are not required to use AI as part of their role, and choosing not to use AI will not be treated as a performance issue. Cruse Scotland will provide guidance to support safe, appropriate use and recognises that uncertainty around new technologies can be challenging.

ETHICAL FOUNDATIONS

Cruse Scotland's approach to AI use is guided by the following principles:

- **Confidentiality:** Client and service user information must be protected at all times.
- **Clinical Responsibility:** Human practitioners retain full professional accountability.
- **Non-Maleficence:** AI use must not increase risk of harm to clients or service users.
- **Transparency:** AI use must not be hidden or misleading.
- **Professional Integrity:** AI must not undermine therapeutic boundaries or relationships.

REVIEW AND POLICY EFFECTIVENESS

This policy will be reviewed annually, or sooner where there are significant changes in the capability and organisational use of AI, safeguarding risk, or legal and regulatory requirements. Effective implementation will be reflected in safe, transparent and proportionate AI use, with no adverse impact on service user trust or safeguarding.

QUESTIONS

Any questions about the content or implications of this document can be addressed to your Line Manager, or the Chief Executive Officer.

POLICY CHANGE SHEET

Date	Change details	Author