# AI Usage Policy Template

Please adapt this template to suit your organisation.

## Purpose

The purpose of this policy is to guide the responsible use of artificial intelligence (AI) by Qlic. This policy aims to ensure that AI is used in a safe, ethical, and socially responsible manner.

## Policy Statement

Our organisation is committed to the responsible use of AI. We will ensure that all AI systems are used in a manner that respects human rights, privacy, and ethical principles.

## Guiding Principles

#### Device Usage: When using company-authorised AI systems, AI systems should only be conducted on a Qlic-provided device. This is to ensure that all information is secured after the fact and that no rogue or malicious software is installed via AI-generated information.

Account Usage: When using company-authorised AI systems, AI systems should only be conducted using a individual Qlic-created account. This allows for Qlic to audit AI usage for quality control, misuse, or rogue responses.

Privacy and Data Protection: Our organisation will protect the privacy and personal data of individuals in all AI-related activities, and ensure that data is collected, used, and stored in compliance with applicable data protection laws and regulations.

Quality Control Risks: AI can generate responses that have little or no value or is false, therefor all responses generated by AI should be cross-referenced against trusted reference points online or reviewed by a member of the team that has expertise in that subject.

Contractual Risks: AI systems should not be used to generate legally binding documents without complete review and sign-off from SMT and/or Qlic legal advise.

Security & Privacy Risks: Using AI can risk exposing confidential and personally identifiable information to unauthorised parties. Qlic needs to be mindful of the data being used in our authorised AI systems to avoid the following but not limited to:

* **Names**
* **Physical Addresses**
* **Email Addresses**
* **Company Confidential Information**
* **Company Identifiable Information**
* **Customer identifiable information**
* **Qlic Systems used**

Intellectual Property Risks: When using an AI system, there is a risk that intellectual property rights could be infringed upon. It is important that any information generated by AI systems are in the public domain and have no IP risks. You should cross reference the information being provided with trusted external sources or be reviewed by a member of the team that has expertise in that subject. This includes the following but no limited to:

* Copyrighted Material
* Government Material
* UK Patented Ideas

Vendor Risks: Many of the risks described above also apply to company data that is provided to or received from vendors. For example, should contracts with vendors specify that information provided by the vendor to the company cannot be generated by AI without prior consent? Should contracts also specify that confidential company data cannot be entered into AI?

## Roles and Responsibilities

All employees, contractors, and third-party partners who are involved in the use of AI systems must comply with this policy. Managers and supervisors are responsible for ensuring that their employees are aware of and comply with this policy.

## Enforcement and Review

Our organisation will regularly review and update this policy as needed to ensure that it remains current and effective. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment.