

Acceptable Use Policy

Purpose and scope

This Acceptable Use Policy (AUP) sets out the rules that apply to all use of the Caldora Compliance platform (the Platform) and its associated services. It applies to the Customer and to all Users authorised by the Customer to access the Platform.

This AUP is incorporated into and forms part of the Caldora Compliance Platform Licence and Subscription Agreement (the Agreement). Capitalised terms used but not defined in this AUP have the meanings given in the Agreement. By using the Platform, the Customer and its Users agree to comply with this AUP.

The purpose of this AUP is to protect the integrity and security of the Platform, safeguard the interests of all customers and users, ensure compliance with applicable law, and set clear expectations for responsible use.

Permitted use

The Platform is designed to help heat network operators, suppliers and related organisations manage their regulatory compliance obligations. Permitted use includes:

- Registering and managing heat network assets within the Platform
- Creating, assigning and tracking compliance tasks and obligations
- Uploading, storing and managing evidence documents and supporting materials
- Using AI-assisted features to generate draft compliance documents and review evidence
- Recording and managing Priority Services Register (PSR) and vulnerable customer data in connection with genuine compliance activities
- Generating compliance reports and downloading platform outputs for internal use
- Inviting and managing team members within your organisation's account

Prohibited use

The following uses of the Platform are strictly prohibited. The Customer is responsible for ensuring its Users are aware of and comply with these restrictions.

3.1 Unlawful and harmful activity

- Using the Platform in any way that violates applicable law or regulation, including UK data protection law, the Computer Misuse Act 1990, or any sector-specific regulatory obligations
- Uploading, storing or transmitting content that is unlawful, fraudulent, defamatory, obscene or otherwise objectionable
- Using the Platform to harass, threaten or harm any individual
- Entering false, fabricated or misleading compliance data with the intention of creating a misleading record or deceiving a regulator
- Using the Platform to facilitate any form of money laundering, bribery or corrupt activity

3.2 Unauthorised access and security

- Attempting to gain unauthorised access to any part of the Platform, its underlying infrastructure, or the accounts or data of other customers
- Probing, scanning or testing the vulnerability of the Platform or its supporting systems without Caldora's prior written consent
- Introducing or transmitting any malware, virus, ransomware, spyware or other malicious code
- Circumventing or attempting to circumvent any authentication, access control or security measure
- Sharing login credentials between users or allowing unauthorised individuals to access the Platform using another user's account
- Using automated scripts, bots or scraping tools to access or extract data from the Platform without Caldora's prior written consent

3.3 Misuse of AI features

- Deliberately submitting false, fabricated or misleading information to the Platform's AI features in order to generate inaccurate compliance documents or manipulate AI outputs
- Representing AI-generated documents as having been independently verified or professionally reviewed when they have not
- Using AI-generated outputs as a substitute for qualified professional or legal advice in high-stakes regulatory decisions without appropriate human review
- Attempting to manipulate, reverse-engineer or extract the underlying AI models or prompts used by the Platform

3.4 Data and privacy

- Entering personal data into the Platform without a lawful basis for doing so under UK GDPR
- Using the Platform to store personal data that is excessive, irrelevant or unconnected to legitimate compliance activities
- Entering sensitive personal data including PSR or vulnerable customer records for any purpose other than genuine compliance management
- Attempting to access, extract or use personal data belonging to other customers of the Platform
- Using the Platform to build or compile data sets for sale, resale or commercial exploitation unconnected to your own compliance activities

3.5 Platform integrity

- Reselling, sublicensing or otherwise making the Platform available to third parties outside your organisation without Caldora's prior written consent
- Using the Platform in a way that places an unreasonable or disproportionate load on Caldora's infrastructure
- Interfering with or disrupting the Platform or its supporting systems or networks
- Reverse engineering, decompiling, disassembling or otherwise attempting to derive the source code of any part of the Platform

- Removing, obscuring or altering any proprietary notices, branding or labels on the Platform or its outputs
- Using the Platform to develop a competing product or service, or to assist a third party in doing so

Customer responsibility for Users

The Customer is responsible for ensuring that all Users within its account are aware of and comply with this AUP. The Customer must:

- Only invite individuals who have a legitimate need to access the Platform as part of the Customer's compliance activities
- Assign appropriate permission levels to each User and review these periodically
- Promptly revoke access for any User who leaves the organisation, changes role, or no longer requires access
- Notify Caldora immediately if the Customer becomes aware of any unauthorised access to its account or any breach of this AUP by one of its Users

A breach of this AUP by a User will be treated as a breach by the Customer.

AI-generated content

The Caldora Compliance platform includes AI-powered features that generate draft documents, analyse evidence and provide compliance suggestions. Users must understand the following when using these features:

- AI-generated outputs are drafts and recommendations only. They do not constitute legal, regulatory or professional advice.
- All AI outputs must be reviewed by a suitably qualified person before being relied upon for regulatory submissions, customer communications or other consequential purposes.
- The Customer and its Users remain solely responsible for the accuracy, completeness and appropriateness of any documents submitted to regulators or relied upon for compliance purposes, regardless of whether they were generated with AI assistance.
- Caldora does not warrant that AI-generated content will be accurate, up to date or fit for any particular regulatory purpose.

Monitoring and enforcement

Caldora reserves the right to monitor use of the Platform for compliance with this AUP. Monitoring may include reviewing usage patterns, access logs and error reports. Caldora will handle any personal data collected in the course of monitoring in accordance with its Privacy Notice.

If Caldora reasonably believes that the Customer or any of its Users is in breach of this AUP, Caldora may take one or more of the following steps depending on the nature and severity of the breach:

- Issue a written warning to the Customer
- Suspend the access of the relevant User or Users
- Suspend the Customer's account pending investigation

- Permanently terminate the Customer's account and subscription in accordance with the Agreement
- Report the matter to law enforcement or a regulatory authority where required or appropriate

Caldora will act proportionately and, where practicable, give the Customer an opportunity to remedy a breach before taking more serious action. However, Caldora reserves the right to act immediately and without notice where a breach poses a serious risk to the Platform, other customers, data subjects or third parties.

Reporting a concern

If you become aware of any use of the Platform that you believe violates this AUP whether by another user within your organisation or otherwise please report it to us promptly at info@caldoracompliance.co.uk. We take all reports seriously and will investigate appropriately.

Changes to this policy

Caldora may update this AUP from time to time to reflect changes in the Platform, applicable law, or best practice. We will notify registered users of material changes by email at least 14 days before they take effect. The current version is always available at caldoracompliance.co.uk/acceptable-use.

Continued use of the Platform after the notice period constitutes acceptance of the updated AUP. If the Customer does not accept the updated AUP, it may terminate its subscription in accordance with the Agreement.

Contact

For questions about this Acceptable Use Policy, please contact us at info@caldoracompliance.co.uk.