

Title	Policy on information security and data privacy
Revision date	04/02/2026
Revision number	1.0
Document reference	CGE-POL-006

Document purpose and scope

This document sets out the **Information Security and Data Privacy Policy** for **Coastal Geohazards Experts Ltd** (“CGE”). It applies to all company activities, including digital publishing, content creation, media production, research, and the operation of online platforms.

The policy covers:

- the Founder
- contractors, freelancers, and collaborators
- any third-party organisations processing information on behalf of CGE

As a micro-enterprise operating primarily through digital systems, CGE recognises the importance of protecting information assets and personal data. This policy will be reviewed annually and made available to relevant stakeholders.

Aim

This policy aims to:

- prevent and minimise the impact of information security incidents
- ensure continuity of operations and protection of digital assets
- comply with legal obligations, including UK GDPR and the Data Protection Act 2018
- maintain high ethical standards and protect CGE’s reputation



Policy on information security and data privacy

- safeguard the confidentiality, integrity, and availability of information

CGE recognises that personal data belongs to the individual data subject and must be handled lawfully, fairly, and transparently.

Policy statement

CGE is committed to maintaining high standards of information security and data privacy. We will:

- comply with all relevant legislation, standards, and best-practice guidance
- protect personal data and other sensitive information from loss, misuse, unauthorised access, or disclosure
- ensure that information is accurate, secure, and available when needed
- maintain proportionate controls appropriate to a digital-first micro-business
- ensure transparency about how data is collected, stored, used, and shared
- expect suppliers, partners, and collaborators to uphold equivalent standards

CGE does not operate an ISO 27001-certified ISMS due to its scale, but adopts the **principles** of structured information security management in a proportionate manner.

Responsibilities

Founder and Director

The Founder holds overall responsibility for:

- implementing and reviewing this policy

CGE-POL-006 Policy on information security and data privacy

Revision: 1.0

This document is classified as PUBLIC



Policy on information security and data privacy

- ensuring compliance with data protection legislation
- overseeing information security risk management
- responding to incidents, breaches, or concerns
- ensuring contractors and collaborators understand their obligations

Contractors, freelancers, and collaborators

Anyone working with CGE must:

- comply with this policy and associated guidance
- protect information they access or process
- report any suspected breaches immediately
- follow secure working practices, including password hygiene and device security

Suppliers and third-party services

CGE relies on reputable digital service providers (e.g., hosting, cloud storage, email, analytics). Suppliers must:

- demonstrate appropriate security measures
- comply with data protection requirements
- process data only under CGE's instruction

Implementation

CGE implements this policy through the following principles:

Top-level commitment



Policy on information security and data privacy

The Founder ensures that information security and data privacy are embedded in CGE's operations and decision-making.

Privacy by design and default

CGE will:

- collect only the minimum data necessary
- use secure, privacy-respecting tools
- apply appropriate access controls
- ensure data is processed lawfully and transparently

Proportionate processes and procedures

CGE adopts simple, effective controls appropriate to its scale, including:

- strong authentication and password management
- encrypted storage and secure cloud services
- regular software updates and device security
- controlled access to information assets

Risk assessment

CGE will:

- identify and assess information security risks
- maintain a simple risk register for digital assets
- conduct data protection impact assessments where required

Communication and training

CGE ensures that:



Policy on information security and data privacy

- contractors and collaborators receive clear guidance
- expectations around data handling are communicated
- individuals know how to raise concerns

Monitoring and review

CGE will:

- review this policy annually
- monitor the effectiveness of security measures
- update practices in line with emerging risks and best practice

Supporting procedures

CGE maintains additional guidance where relevant, including:

- secure password practices
- acceptable use of digital tools
- data retention and deletion procedures
- incident reporting and breach response

Approval

This policy is approved by:

Founder & Director Coastal Geohazards Experts Ltd on 04/02/2026

Andres Payo

Director