



Digital Privacy and Safety Standards

September 2026

1. Purpose

These Standards establish practical expectations for responsible use of digital systems, information and communications associated with Pinion Institute.

They operate alongside the **Privacy Policy**, **Community Participation Agreement**, **Code of Conduct** and other applicable Institute policies.

Pinion Institute seeks to manage digital information responsibly and proportionately to the nature and scale of its activities.

2. Personal Information

Personal information should be collected, accessed, used and retained only where reasonably required for Institute or business purposes.

Access to personal information should be limited to those who have a legitimate need for it.

Personal information must not be sold, harvested or used for unrelated marketing, profiling or other purposes without appropriate authority.

The handling of personal information is further addressed in the Institute's **Privacy Policy**.

3. Member and Community Information

Information available through restricted member or contributor spaces should be treated according to the level of access intended for that environment.

Participants must not, without appropriate permission:

- redistribute restricted member information;
- circulate screenshots or recordings from restricted spaces;
- disclose another person's private contact or profile information;
- use member information for unsolicited commercial or other unrelated purposes;
- attempt to obtain access to material for which they have not been authorised.

Members remain responsible for exercising reasonable care about information they choose to share with others.

4. Account and Access Security

People given access to Institute-controlled digital systems should:

- use their own authorised account;
- keep passwords and access credentials secure;
- not share restricted login details;
- notify Pinion Institute if they reasonably suspect unauthorised access to their account;
- comply with access limitations applying to particular resources or areas.

Access may be changed or withdrawn where necessary for security or responsible administration.

5. Digital Communications

Communication through Institute-controlled platforms should comply with the **Code of Conduct**.

Participants must not use Institute systems to:

- harass or threaten others;
- impersonate another person;
- distribute malicious or unlawful material;
- deliberately compromise another person's privacy;
- circumvent access controls;
- conduct unauthorised commercial solicitation.

Private or restricted communications must not be recorded, reproduced or distributed without appropriate authority.

6. Intellectual and Creative Material

Digital availability does not mean that material is free to copy or reuse.

Participants must respect copyright, licences, attribution requirements and any access restrictions applying to:

- research;
- publications;
- manuscripts;
- educational resources;
- images;
- recordings;
- presentations;
- creative work;
- other material made available through Pinion Institute.

Ownership and permitted use of intellectual property are addressed more fully through the Institute's applicable IP, publishing and contributor arrangements.

7. Artificial Intelligence and Automated Tools

Artificial intelligence and automated tools may be used where appropriate, but their use must remain consistent with:

- privacy;
- confidentiality;
- copyright;
- intellectual and academic honesty;
- research integrity;
- applicable permissions.

Restricted, confidential, unpublished or personally identifying information must not be entered into an external AI or automated system without appropriate authority.

Institute or member content must not be scraped, harvested or used to train external systems without permission.

Responsibility for material produced or submitted with the assistance of AI remains with the person using it.

8. Service Providers

Pinion Institute relies on third-party digital services, including Wix and services connected with the operation of its website, members area and online store.

Where information is processed through such providers, their systems and privacy practices may also apply.

Pinion Institute should use available security and privacy controls reasonably appropriate to its activities and should review significant service arrangements where circumstances materially change.

9. Digital Incidents

Suspected:

- unauthorised access;
- loss or disclosure of personal information;
- compromised accounts;
- malicious activity;
- serious privacy breaches;
- significant security incidents

should be reported promptly to the Founder and Director.

Immediate steps may include securing an account, changing credentials, restricting access, preserving relevant information and contacting the relevant service provider.

Significant personal-information incidents are dealt with under the **Data Breach Response Plan**.

10. Review

These Standards should be reviewed when significant changes occur in:

- the Institute's digital platforms;
- member functions;
- information handling;
- technology use;
- legal obligations;
- significant security risks.

Document: Digital Privacy and Safety Standards

Responsible role: Founder and Director

Version: 1.0

Date adopted: 09/26

Review date / trigger: 09/27