Information Security Policy

Last Reviewed: April 2024

This is an overarching policy which explains the main ways in which Sylva Foundation ('we/us/our') ensures the secure handling of data and information while providing appropriate access.

It applies to everyone: all staff, trustees, associates, contractors, volunteers, and anyone else authorised to use Sylva Foundation IT facilities and information ('users').

Policy

Sylva Foundation's policy is that the information it manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

1. Sylva Foundation will aim to achieve a culture in which legal requirements and information security risks are considered whenever information is handled, through the provision of training, awareness campaigns and specialist guidance and advice.
    a. All information users will be appropriated inducted, trained and supported.
2. Sylva Foundation will implement information security management practices which apply appropriate security while at the same time enabling users, to access and use the information they need.
    a. Controls will be put in place which control access to and use of certain information.
3. Sylva Foundation will collect, store and process information in accordance with applicable laws and according to its Data Protection Policy.
4. Information held in user accounts may be examined on behalf of Sylva Foundation by authorised persons for specific operational or legal reasons.
5. Sylva Foundation will strive to ensure excellent site security standards.
    a. We will undergo an annual certification with the government-backed Cyber Essentials system.
6. This document, should be read in conjunction with other key documents (see Related documents/procedures).

Scope

This policy is binding on all those who use Sylva Foundation information ('users') including: staff, trustees, contractors, consultants, associates and volunteers.

This policy applies in all locations and devices, whether accessing information via IT equipment at the Sylva Foundation premises or elsewhere including mobile devices.

This policy supplements the Sylva Foundation Protection Policy.

Oversight

Overall responsibility for information security at Sylva Foundation is delegated from the trustee board to the Chief Executive, who has the authority to define and implement organisation-wide information security policies.

The Chief Executive is supported by the organisation's Head of Web Development, and reliant upon him/her for good advice received on matters of a technical nature.

Certain third-parties provide additional support and/or advice, notably an annual site security audit delivered under our Cyber Essentials certification.

Responsibilities

All information users are responsible for protecting and ensuring the security of the information to which they have access.

Project managers are responsible for ensuring that all information in their area is managed in conformance with this policy.

All users who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

Any breach of information security or violation of this policy must be reported to the Chief Executive who will take appropriate action and inform the relevant authorities.

Related documents/procedures

- Information Map
- Data Protection Policy
- Privacy Notice – online services
- Service Terms – online services
- Information Commissioner's Office (ICO) registration. Our Registration Number is **Z1773491**.
- Site security certification with Cyber Essentials

Review

This policy will be reviewed annually. Last updated as shown at the top of the document.