**Taith Confidentiality Policy**

|  |  |
| --- | --- |
| **Purpose of document** | To outline the process for reporting and handling personal data breaches. |
| **Version** | 1 |
| **Issue date** | June 2023 |
| **Revision date** | June 2024 |

**1. Purpose**

The purpose of the policy is to set out expectations for how Taith will handle confidential information.

**2. Scope**

This policy applies to staff and any other party handling information for which Taith owes a duty of confidence.

**3. Relationship with existing policies**

This policy should be read in conjunction with the [Cardiff University Information Security Policy](https://www.cardiff.ac.uk/public-information/policies-and-procedures/information-security).

It also has a relationship with other Taith policies specifically:

* Taith Data Protection Policy
* Records Management Policy

**4. Policy statement**

4.1 Taith holds confidential information (See section 7 - Definitions) about individuals and other non-personal confidential information, e.g. information about business finances, strategy and planning.

4.2 Staff are under a common law obligation not to disclose confidential information inappropriately, whether it relates to people or otherwise.

4.3 Staff are also contractually obliged to maintain ‘mutual trust and confidence’ with Taith and not to disclose confidential information without proper authorisation.

4.4 Anyone processing personal confidential information (e.g., transcribers, consultants) on behalf of Taith must only do so under contract.

4.5 Deliberate or reckless breaches of confidence relating to confidential information held by Taith may be treated as a disciplinary offence and may constitute an offence under Data Protection law. Such breaches may also be actionable by the party whose confidence has been broken and result in litigation against the individual who breached the confidence.

4.6 All staff should ensure that they have undertaken Cardiff University’s compulsory information security training (available through their learning central account).

**5. Responsibilities**

All staff should ensure that any confidential information concerning Taith business for which they are responsible is stored securely in line with [Cardiff University’s Information Classification and Handling Rules](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.cardiff.ac.uk%2F__data%2Fassets%2Fword_doc%2F0004%2F2728858%2FInformation-Security-Classification-and-Handling-Policy-v-4.1-FINAL-EN.docx&wdOrigin=BROWSELINK) and in such a way that confidentiality is maintained.

**6. Compliance**

All alleged breaches of confidentiality shall be notified to the Taith Senior Project Manager as per the Taith Data Breach process. Any infringement by staff may expose Taith and/or the individual to legal action, claims for substantial damages and, in the case of confidential information containing personal data, fines from the Information Commissioner.

Any infringement will be treated seriously by Taith and may be considered under relevant disciplinary procedures.

**7. Key definitions**

***Confidential Information***

Confidential information is defined in categories C1 and C2 of [Cardiff University’s Information Classification and Handling Guidelines](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.cardiff.ac.uk%2F__data%2Fassets%2Fword_doc%2F0004%2F2728858%2FInformation-Security-Classification-and-Handling-Policy-v-4.1-FINAL-EN.docx&wdOrigin=BROWSELINK) and includes any information to which the common law ‘duty of confidence’ applies. A duty of confidence is created when ‘private’ information has been passed on in such a way that the person receiving the information was aware, or should have been aware, that the information was being imparted on the basis of confidentiality. (The legal test is whether a ‘reasonable’ person would think the recipient ought to have known that the information was confidential).

***Personal Data***

Confidential information may include personal data which is any recorded information about a living individual who can be identified from that data or from that data and other available data. This includes, inter alia, information held in paper records, electronic records, digital files, video and audio recordings, photographic images.

|  |  |
| --- | --- |
| **Document name** | Confidentiality Policy |
| **Version** | 1 |
| **Issue date** | December 2023 |
| **Revision date** | December 2024 |
| **Policy owner** | Data Protection Officer |
| **Policy author** | Data Protection Officer |
| **Approval date** | 21 December 2023 |
| **Approved by** | Susana Galván |