**Ted Lewis Centre Charity No. 1199771**

**Confidentiality Policy**

Date originally approved 22 September 2020.

Reviewed T Bartlett, Chair on 5th February 2022 with no alterations.

Reviewed Trustees 5th December 2023

Reviewed

Reviewed

**The Ted Lewis Centre Confidentiality Policy**

**Policy Statement and Purpose:**

We define Organisation Members as Trustees, members, paid staff and volunteers. Centre is the Ted Lewis Centre Charity no 1199771

This Confidentiality Policy explains how we expect our organisational members to treat confidential information. Organisation Members will from time to time unavoidably receive personal and private information about other organisational members, external parties including donors, and visitors.

Information must be protected for three reasons:

* Be legally required (e.g. sensitive data); or
* concern for organisation’s financial data including donations received; or
* concern for potential partners; and
* in compliance with General Data Protection Regulation (GDPR), the legal framework which sets guidelines for the processing of personal data and information.

**Scope:**

This policy affects all Organisation Members who have access to confidential information.

**Policy Elements:**

Confidential information is secret, valuable, expensive or easily replicated. Common examples of confidential information are:

* Unpublished financial information
* Data of Partners/ Visitors/ Financial Donors (existing and potential)
* Organisational members’ lists (existing and potential) with personal contact data
* Data entrusted to our organisation by external parties
* Documents explicitly marked as confidential
* Unpublished goals/ forecasts/ initiatives marked as confidential

Organisation Members may have various levels of authorised access to confidential information. These are set out in Schedule 1

**What Organisation Members should do:**

* Lock or secure confidential information and documents at all times whether in the Centre or off-site.
* Shred confidential documents wherever possible when no longer needed.
* Be aware of what people have access to confidential information in accordance with Schedule 1
* Make sure that the Centre approves the use of access by way of private electronic devices not in the day-to-day control of the Centre.
* Ensure that confidential information is only accessed on secure devices.,
* Only disclose information to other colleagues and members when necessary and when authorised to do so.

**What organisation members should not do:**

* Use confidential information for any personal benefit or gain.
* Disclose confidential information to anyone outside of our organisation without the express permission of the Trustees.
* Replicate confidential documents and files and store them on insecure devices.

**Confidentiality Measures:**

To ensure that confidential information is well protected, organisation members will as appropriate:

* Store and lock paper confidential documents.
* Encrypt, where appropriate, electronic information and safeguard databases.
* Ask for authorisation from the Trustees to allow any other organisation member(s) to have access to certain confidential data and information as may be required and/or appropriate.
* Ensure that any electronic communication devices capable of accessing the Centre’s records and operated by Confidential Members which contain confidential information are maintained to proper degrees of Cyber Security sufficient to safeguard the Centre against any breaches of GDPR.

**Exceptions:**

Confidential information may have to be disclosed for legitimate reasons. Examples are:

* If a regulatory body requests it, as part of an investigation or audit
* If our organisation examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, organisation members involved should document their disclosure and collect all authorisations needed. All organisation members should not disclose more information or data than needed.

**Disciplinary Consequences:**

Every suspected breach of this policy will be investigated thoroughly whether intentional or unintentional.

* If any member of the public or Organisation Member of the Centre believes that there has been a breach of confidentiality, this must be reported to the CEO as soon as practicable, and he or she will make a record of this report in hard copy of electronically.
* The CEO is responsible for the investigation but if it is the CEO who is alleged to have broken confidentiality, the Chairman of the Trustees will be so responsible.
* A record will be kept of the investigation, the outcome and its communication to the informant who will be advised of his or her right to appeal to the Information Commissioner.

Organisation members who breach this Confidentiality Policy wilfully or for personal gain will face a disciplinary hearing held before at least two members of the Board of Trustees. Resulting action taken may include legal action in extreme cases.

Any unintentional breach of this policy will be dealt with by the CEO and appropriate action taken and recorded.

This policy is binding on all organisational members current or past.

**Training.**

The Centre will provide appropriate training from time to time for its Organisation Members as to the requirement for compliance with GDPR, the provisions of Schedule 1 and in the necessity for ensuring a proper degree of Cyber Security.

Every Organisation Member will sign the Centre’s Privacy Policy

Schedule 1

|  |  |
| --- | --- |
| Type of Organisation Member or other body, company or concern | Level of access to confidential information. |
| Trustee | All personal information of volunteers, visitors and other Trustees that has been disclosed as part of the legitimate operation of the Centre |
| Volunteer | Personal information of visitors only |
| Staff | Personal information necessary for them to undertake their duties with the consent of the CEO |
| Contractors | None |
| Community organisations | None unless approved by the person about whom the information is about |
| Statutory bodies | Information statutorily required or compliant with GDPR |

Initially Adopted by the Ted Lewis Centre on September 2020, reviewed 5 February 2022 and

To be reviewed every 2 years

Confpolicy201123