Working Together Ludlow

to include people with learning difficulties

Date Policy Adopted by the Board of Trustees:	**February 2020**
Policy Review Date:	**February 2022**

Confidentiality Policy

Working Together recognises that the legitimate use of confidential information underpins our service. All information about our members is treated as confidential, to be shared only as necessary in support of their needs.

Working Together ensures that personal and operationally sensitive information is maintained confidentially by the charity. Any disclosure of confidential information about a member to another person for the purpose of assisting the member is only undertaken with the expressed permission of the member and/or their parent/s or carers, *except* To protect the welfare of a child or vulnerable adult *or* In very limited and extremely rare circumstances where a person is suspected of a disclosable offence or terrorism.

Working Together's position on confidentiality is made clear to all connected with it.

The Chief Officer and Trustees of Working Together are responsible for ensuring that the requirements of this policy are met throughout the charity's services. Breaches of confidentiality are treated seriously and may result in the individual concerned being required to leave the organisation.

All new trustees, employees and volunteers are provided with a copy of the Working Together Confidentiality Policy as part of their induction / training. All are expected to abide by this policy and procedures.

Confidentiality Procedures

Personal, Financial and Sensitive Information

Personal, financial or sensitive information, whether in hard or soft copy form, should only be accessed by staff to the extent necessary for the performance of their duties at Working Together.

Personal, financial or sensitive information, whether in hard or soft copy form, should not be held by any staff member outside Working Together premises, save to the extent necessary for the carrying out of Working Together's business or activities in a lawful, proper and efficient manner.

Personal, financial or sensitive information so held is the responsibility of the individual holding it.

Personal, financial or sensitive information, whether in hard or soft copy form and wherever held, should not be left unattended or visible in a public place when in use and must be stored securely when not in use. For example, personal plans for use at a project session will need to be accessible to all staff, if needed, but should be kept out of sight and not within easy reach of members or their families. They should be stored in a place and manner such that they cannot be accidentally moved or mistakenly taken by others. If possible, there should be a secure cupboard or drawer at each setting for this purpose which can be locked or otherwise safely protected.

Any loss of personal, financial or sensitive information or suspected loss of information, in whatever form, must be reported as soon as practicable to the Chief Officer, or, in their absence, the Chair of Trustees.

Personal, financial or sensitive information, in whatever form, must not be disclosed to anyone outside Working Together save as referred to below.

Disclosure of information outside Working Together Ludlow

Personal information must not be disclosed outside Working Together unless those to whom it relates gives their consent for its use for the specific purpose concerned, or unless its disclosure is required by law or other regulatory requirements.

Financial information must not be disclosed outside Working Together, without the consent of the Chief Officer or the Chair of Trustees or as required by law or other regulatory requirements.

Sensitive information must not be disclosed outside Working Together unless those to whom it relates give their consent for the specific purpose concerned or its disclosure is required by law or other regulatory requirements.

Sharing sensitive information

In the context of safeguarding children and safeguarding vulnerable adults from abuse, sensitive information may need to be shared as provided for in Working Together's Safeguarding Policies and Procedures.

Staff should refer to the relevant policy and procedure if they feel sensitive information needs to be shared in any given case. In any event, save in cases of emergency, staff must refer to the Chief Officer, as the nominated responsible person for safeguarding for guidance, or the Chair of Trustees or Nominated Trustee with responsibility for Safeguarding.

Avoiding casual disclosure of information

All staff are required to take all reasonable measures to ensure that:

- when using any personal, financial or sensitive information, in whatever form and in whatever circumstances, such information is not seen by any person who is not authorised to see it,

  and

- when discussing any personal, financial or sensitive information, in whatever circumstances, such information is not heard by any person who is not authorised to hear it.

Return of all documentary information

All documentary information, whether in hard or soft copy form, given to or acquired or created by any staff member in the course of and relating to their working with Working Together must be returned to Working Together Ludlow at the end of the working relationship.

Security of Information

It is the policy of Working Together Ludlow to have in place operational measures to ensure that information relating to its business and activities is kept secure and in a manner consistent with current law, regulatory requirements and recommended practice.

The Chief Officer has day to day responsibility for information security measures. All staff members are responsible for ensuring that all personal, financial and sensitive information with which they may come into contact in their work with Working Together is kept secure by them in accordance with the law and with these policies and procedures, and are required to report any matters of concern relating to the security of such information to the Chief Officer, or Chair of Trustees in their absence, as soon as practicable.

Information in hard copy form

Personal, financial and sensitive information in hard copy form, wherever held, is required, when not actively being used, to be kept in locked drawers/filing cabinets/cupboards, with access to relevant keys and knowledge of their location being restricted to staff who may need access to such information to carry out their duties.

When in use, this information should be out of sight, and if possible, in a locked or secured place where there is minimal chance of members, families, volunteers, the general public or others being able to remove it, whether accidentally or on purpose.

All such information when being taken from one place to another is required to be kept under the direct control of the person responsible for it in as secure a manner as is practicable in all the circumstances.

No such information should be posted unless authorised by the Chief Officer or Chair of Trustees for the efficient running of Working Together's business and activities.

Original documents of which no copy exists should, wherever reasonably practicably, be copied before posting.

Information held electronically

Personal, financial and sensitive information in electronic form must be subject to password access for individual authorised users only, authorisation being restricted to staff who may need access to such information to carry out their duties.

All such information when being taken from place to place, in particular on any portable equipment or media (such as laptops, tablet computers, memory sticks and memory cards), is required to be kept under the direct control of the person responsible for it in as secure a manner as is practicable in all the circumstances.

All smart phones, laptops and tablets must have a secure password or code that is necessary to turn on and use the device in addition to the passwords needed prior to using any online IT system and the passwords attached to the files or data storage system themselves.

Equipment or media containing any such information must not be posted under any circumstances.

Retention and disposal of information

Personal, financial and sensitive information, in whatever form, will be held for such period, depending on its nature, as complies with recommended practice on retention of information.

In particular, information relating to any safeguarding issue will be kept indefinitely and financial information will be kept for a minimum of 7 years.

Personal, financial and sensitive information in hard copy form will be shredded.

Personal, financial and sensitive information held electronically will be deleted from the relevant equipment and media.

Equipment and media which has contained personal, financial or sensitive information will be disposed of in such manner as ensures that any residual information is securely deleted during the disposal process.

More information can be found in our Data Protection Policy.