

## Confidentiality Policy

### Scope

This policy applies to all members of CANDI's staff – employees, volunteers, management and trustees. CANDI aims to provide a completely confidential service, subject to any safeguarding issues.

Employees, volunteers and trustees will:

- keep anything told to them by anyone of any age in strict confidence.
- will not discuss any information about individuals with anyone else, unless asked to by the individual concerned.
- In very exceptional circumstances, if personal safety or that of another person is at risk, tell someone else, but will tell the individual exactly what is happening.

### Principles

All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either the Chair of Trustees or the Safeguarding Trustee.

### Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons.

### Document control

Last updated	10 September 2024
Next review	14 September 2027