

Title of policy:	Confidentiality Policy
Original Date of issue	August 2012
Date of issue:	August 2024
Version:	7.0
Author:	Chief Executive Officer / HR
Owned by:	Chief Executive Officer / HR
Approved by:	Board of Trustees
Date of next review:	June 2024

Related policies, procedures and guidance:

Adult Safeguarding
Child Protection
Data Protection Policy
Disciplinary Policy
Electronic Information and Communications Policy
Privacy Notice

POLICY STATEMENT:

This policy is written to set out Carers in Bedfordshire's commitments to, and responsibilities for confidentiality. This is a discretionary policy, which does not form part of a contract of employment. The Board of Trustees of Carers in Bedfordshire may vary or amend the policy as it deems necessary.

The term staff is used in this document as a generic statement to refer to any person working for Carers in Bedfordshire in any capacity and includes volunteers, part time staff, Board members, sessional/ temporary workers and placement students.

All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. All clients information must be treated with complete confidentiality and MUST NOT be divulged to anyone who does not have the right to access. Information refers to ALL information including that held on paper, in manual form and electronically. Access to information on clients is restricted to those who have been given permission by the client, except in specific circumstances laid out in this policy and guidelines.

1. PURPOSE

CIB are committed to safeguarding the confidentiality of the individual and the information it holds about them.

This policy has been produced to:

- Inform staff of the need and reasons for keeping all personal and commercially sensitive organisational information confidential.
- Inform staff about what is expected of them.
- Ensure the organisation complies with its duty as an employer and as a provider of services that requires handling confidential information in order to deliver that service.

2. POLICY

2.1 Introduction

All staff working for CIB are bound by a legal duty of confidence to protect the personal information that they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 2018 which is the UK's implementation of General Data Protection Regulation (GDPR).

All staff of the organisation come into contact with confidential information at some level on a regular basis and as such need to be aware of their personal responsibilities to its use and protection.

Clients expect that their personal and sensitive information will be treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff/volunteers.

Volunteers are also bound by a duty of confidence when volunteering within the organisation. The organisation must ensure that volunteers are not placed in a position or given a task that allows them access to data beyond that which they need to fulfil their role.

2.1 Principles of Confidentiality

Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent. Confidential information may include personal information such as name, age, address and personal circumstances, as well as sensitive personal information regarding race, health, sexuality, etc.

Clients have a right to expect that CIB staff in will not disclose any personal information learnt during the course of their duties, unless permission is given. Without assurance about confidentiality clients may be reluctant to give information that may be required in order to provide care.

Similar considerations apply to personal information concerning individuals, such as staff, donors and volunteers.

Confidential information may be known, or stored on any medium. Photographs, videos etc. are subject to the same requirements as information stored in records, on a computer, or given verbally. Information that identifies individuals personally must be assumed to be confidential, and should not be used unless absolutely necessary. Whenever possible, anonymised data (from which personal details have been removed and which therefore cannot identify the individual) is to be used instead. Note however that even anonymised information can only be used for justified purposes.

2.2 Awareness and Compliance

Everyone at CIB must be aware of the importance of confidentiality. All staff must be aware of their responsibilities for safeguarding client confidentiality and keeping information secure. It must be remembered that no individual within the organisation has an automatic right of access to personal information held by CIB.

Staff must comply with requirements of the Data Protection Act 2018 (GDPR) and the Freedom of Information Act 2000. Breaches of confidentiality are a serious matter and non-compliance with this Policy may result in disciplinary action being taken.

On joining the organisation new members of staff will be asked to sign up to the Data Protection and Confidentiality Policy.

All volunteers are asked to sign that they have read and understood the Confidentiality Policy when they start with the organisation. In addition, all volunteers are reminded in their placement about the importance of confidentiality. From time to time updates around confidentiality are circulated via the volunteer co-ordinator.

2.3 Responsibilities

No member of staff shall knowingly misuse any information or allow others to do so. Any breaches/potential breaches of confidence are to be reported to the Quality Officer and will be discussed by the Board.

It is important that individual responsibilities towards the maintenance of confidentiality are known and understood:

- The Board is responsible for overseeing and advising on issues of client confidentiality for CIB.
- The CEO and Leads are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information within individual areas e.g. departments.

Individual staff are:

- Responsible for maintaining confidentiality. This duty of confidentiality is written into contracts. Breach of confidentiality of information gained, either directly or indirectly in the course of duty will be considered a disciplinary offence that could result in dismissal.
- Authorised only to have access to personal information they need to know in order for them to perform their duties. Gaining access or attempting to gain access to information for any other purpose will be seen as a breach of confidentiality as passing information on to someone who is not authorised to receive it.
- Responsible for safeguarding the confidentiality of all personal and organisation information to which they have access, this includes its safe and secure transfer and storage.
- Personally responsible for any decision to pass on information to another person/third party.
- Responsible for adhering to the Confidentiality Policy, the Data Protection Act 2018.
- Also expected to treat any non-person identifiable information that could be considered sensitive to the business of the Charity with the same degree of care as would be afforded to person identifiable information.
- Guidance and support relating to the maintenance of confidentiality and security of information is available in the form of the Confidentiality Policy and from the Board and CEO.
- Our finance software and fundraising data contain confidential information relating to individuals, and the Charity. Information held within these databases is to be accessed and shared according to individual's roles and should only be accessed and shared on a need to know basis in accordance with the Data Protection Act 2018 (GDPR).

2.4 Acting on the Duty of Confidentiality.

Any personal, sensitive or financial information, must be treated as confidential.

No personal information, given or received in confidence, may be passed to another person or organisation without the consent of the provider of the information. This is usually the client but sometimes another person may be the source (e.g. relative or carer).

No personal information, given or received in confidence for one purpose, may be used for a different purpose without consent of the provider of the information this is the same with donors.

Whilst clients usually understand and accept that information may be shared within the CIB team in order to provide services, it is still necessary to check that the client understands what will be disclosed and who may be contributing to their support.

It is also important to respect the wishes of any clients who object to their information being shared, except where this would put others at risk of death or serious harm.

The overriding principle is that clients, donors, staff or volunteers should not be shocked to find out how their information has or is being used or shared, rather that they should be effectively informed to allow them to exercise their rights in relation to their data.

Any decision to break confidentiality without the consent of the individual concerned must be authorised by a Lead, or another appropriate senior member of staff.

When requests are made by the police or any other official agency for information these must be referred to the Data Protection Officer who is the Chief Executive Officer or their appointed deputy. Such requests are not normally accepted unless they are in writing and provide a full justification for the breach of confidentiality.

It is only in relation to these exceptions and to witness summons to appear in Court that information must be disclosed.

Where a member of staff or volunteer is seeking advice and support they may share relevant information with their manager or the Data Protection Officer. The duty of confidentiality must then be maintained by both of them.

All matters of a confidential nature discussed by the Board of Trustees must be kept within the Board. Trustees are not permitted to discuss confidential matters outside the organisation unless approval in each individual case has been sought and granted by the rest of the Board.

2.5 Training and Awareness

Training and awareness of the importance of the maintenance of confidentiality and information security will be an ongoing process throughout an individual's employment with CIB and will form part of the mandatory training programme.

Leads will be responsible for ensuring that staff are made aware of any specific departmental requirements/procedures.

2.6 Monitoring

The CEO will provide regular reports to the Board, such reporting to include the number of reported 'information' untoward incidents including:

- breaches or near misses of confidentiality, security or misuse of data
- staff training undertaken



CONFIDENTIALITY AND NON-DISCLOSURE DECLARATION

While working as an employee, director/trustee, volunteer, partner or contractor of Carers in Bedfordshire, you may hear confidential information concerning carers and their personal lives and/or information concerning the work or plans of the charity which may be commercially sensitive.

This information should be shared only with the Carers in Bedfordshire team members with whom you are working.

I declare that I will uphold the confidentiality of all information disclosed to me by Carers in Bedfordshire.

Name.....

Signed.....

Date.....