Cumberland Council

C5 Confidentiality

Version: New

Date: 01/04/23

Extra Care Housing Servce	Support at Home Service	OA Day Services	Residential Services	DMH Day Services	DMH Supported Living Services	Community Equipment Services	Shared Lives Service
✓	✓	✓	✓	✓	✓	✓	✓

Policy

To ensure staff maintain appropriate levels of confidentiality.

General Principles

Staff must not share or discuss any information outside of appropriate work-related forums, meetings, procedures or recording systems.

Where it is necessary to share information, this should be done with the consent of the individual or, where this is not achievable, it can be clearly demonstrated to be in the best interest of the individual and the reasoning must be recorded. This includes both written and verbal information.

Where it is necessary to hold a work discussion staff must always be aware of their surroundings e.g., mobile phone and open plan office.

Service User Request for Confidentiality

An individual requesting absolute confidentiality when disclosing information or discussing specific issues should be informed that this cannot be guaranteed. If the content of the discussion includes any allegation or suggestion of abuse / mistreatment it will be necessary to share this information with senior staff members, health care professionals and the safeguarding team.

Where a service user is a relative of a member of staff the staff member must inform the line manager.

Electronic information such as care planning can be locked down at the request of the service user / family if required. Access to confidential information is restricted to those council staff who for the purpose of their role and responsibilities and ensuring it is proportionate to their job role will be given the correct level of access. This can however be locked down where a manager or senior manager request it.

Staff or Service User Files

The content of staff or service user files should be considered as confidential and appropriate steps taken within individual provider units to maintain effective security.

When not in use staff or service user files must be secured in a lockable facility and access restricted to appropriate persons.

Where information is kept in a service users home the service user will take responsibility for this. This must be discussed with the service user prior to the admission process.

Access to Service User Files

Access to service user files should be restricted to the following:

- Service user who will, where necessary, be provided with support to interpret the file / Electronic information content appropriately.
- Service user representative, e.g., an individual whom the service user recognises as advocating on their behalf.

- Council staff members and allocated health care professionals requiring access for reference information gathering or recording purposes.

Access to Staff Files

Access to staff files should be restricted to senior / administration staff in line with their duties. Staff files may be accessed for audit purposes or as part of other Council procedures.

Breaches of Confidentiality

Staff should be aware that any breach in confidentiality may be considered an act of gross misconduct, potentially resulting in disciplinary procedures being implemented.

Training

It is the belief of Care Services training facilitators that the use of teaching methods which include the discussion of actual workplace practice and procedures can result in improved learning outcomes. These discussions should be treated as confidential and should not be discussed outside the training arena.

Care Services training facilitators are committed to the reporting of inappropriate practice (including that of inappropriate attitudes and values), which may be evidenced as a result of:

- Disclosure by service users or employees
- Training facilitator's observation
- Information to be reported will be communicated through the appropriate line management route and the training team in accordance with appropriate policy and procedure where available.

For further information see Council Guidance:

- Data Protection
- GDPR / Information security
- Caldicott Principles