



CP 03 - Confidentiality

Purpose

The aim of this policy is to ensure that all individuals have confidence in knowing that information regarding them will not be disclosed to another individual(s) without prior consent. When an individual is unable to give consent due to lack of capacity, the principles of the Mental Capacity Act 2005 will be adhered to.

All employees will be reassured to know that information regarding them will not be disclosed unless prior consent has been given.

Winash Rest Home will also have the same confidence regarding its business and all company information.

To comply with General Data Protection Regulations (GDPR)

Policy Statement

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

Confidentiality is essential to trust between all individuals and it is Winash Rest Home's purpose and responsibility to ensure that trust is not violated by breaches of confidentiality.

Procedure

All staff are to read and signify that they understand the following policies and procedures at induction and periodically throughout their employment:

- GDPR
- Record Keeping
- Confidentiality
- Mobile phone, social media and internet

All information must be considered by staff to be confidential. The information known by staff concerning individuals must only be discussed in the course of their professional duties and not as a matter of idle or informal conversation.

All staff to be aware that breaches in confidentiality will incur the disciplinary procedure and may lead to dismissal.

All individuals will have their rights to privacy and dignity upheld.

Staff are not to discuss Residents with other Residents, unless they are specifically requested to do so by the Manager.

When receiving requests for information about Residents over the phone it is best to ask the person who they are and then ask the Resident what information they wish to give. Alternatively, ask the person in charge how much information it would be appropriate to share.

Personal information should not be divulged about Residents / Staff without their prior consent, this includes giving out home telephone numbers.

Information about Winash or Residents should not be discussed outside the home.

Hard copy records about Residents are to be locked away either in the Front office or back office.

The computerised records on Caredocs are password protected, staff should not tell people their passwords. Caredocs should be logged out from at the end of completing records.

Verbal handovers should be carried out in a private area, where it cannot be overheard.

During the care planning process, consent will be sought from individuals for the sharing of information with colleagues and relevant professional agencies on a need to know basis. Consent permission will be reviewed regularly. Should an individual lack the capacity to give consent, then the procedures for Best Interest Decision will be implemented as per the Mental Capacity Act 2005.

Due to the nature and complexity of care given to individuals, assurances cannot not be given to individuals that information they give about themselves will be handled by the same staff to whom it was first passed; however, assurances can be given that information is only seen by staff who have valid reasons for accessing that information.

Occasions may arise where an individual passes information to a member of staff requesting that no one else must be informed. In this situation, the member of staff must warn the informant that any information received that has an adverse implication for the welfare of another individual, or the reputation of the company, must be passed to the management. Therefore, the information could only be accepted on this understanding.

All persons should be aware that Winash Rest Home can only maintain confidentiality where it does not conflict with its legal responsibilities to Government laws and CQC regulations and it may be required to disclose certain information as per the Safeguarding and GDPR policies.

All confidential information that is referred to in training or group sessions will be discussed with respect and caution and in ways which conceal the identity of the individual to whom it relates.

All company information is sensitive and includes all financial data, company strategies, employee information etc. and is considered to be confidential and therefore must not be shared inappropriately.

When an individual leaves the service or the organisation, the need for confidentiality continues and therefore personal data and/or company information must not be divulged to a third party for any reason.

Breaches of Confidentiality are dealt with as a Disciplinary Matter