**CONFIDENTIALITY POLICY AND PROCEDURE**

**Purpose**

• To ensure that sensitive information is only shared for the purpose of a Service User's wellbeing such as ensuring the smooth running of a medical procedure or protecting the person from abuse.

• To ensure that all information is collected, recorded, stored, shared and disposed of in the best interests of the

Service User and staff with regard for their human rights and in line with legislation.

• To ensure Zenith Care User and staff are aware of the organisation’s confidentiality policy and procedure.

**Scope**

• All staff and everyone involved in the care or support of Service Users.

**Policy**

• Zenith Care User's rights to confidentiality must be safeguarded in accordance with the common law duty of confidentiality and Article 8 of the Human Rights Act 1998. Zenith Care employee will use information only in the best interests of Zenith Care User and where possible with their express consent.

• All information about Service Users and staff, verbal, written, electronic or photographic *I* video *I* audio recording is managed in line with the Data Protection Act 1998.

• Confidential Information should be shared in line with the Caldicott Principles 1998.

• Information about Service Users may also be covered by the Access to Health Records Act 1990. Procedure

**Verbal Exchange of Information**

• In order for staff teams to work consistently with the people they support, it is necessary for verbal information to be exchanged.

• This may take the form of "team meetings", or "handovers". Zenith Care must provide areas where these activities can take place without being overheard.

• Staff will be trained and advised to only conduct discussions in private areas with people who "Need to Know" the information in connection with their work with Zenith Care User.

• Verbal breaches of Confidentiality will be treated with the same seriousness as a written breach.

**Data Collection and Storage**

• Staff must ensure that any information collected and stored is limited to that which is essential for the care and safeguarding of Zenith Care User. This relates to personal data and health information essential to establish individual needs and provide staff with the means to plan care and support.

• Any information collected and stored about staff is limited to the essential information needed for their employment with the organisation.

• Staff must retain information and data securely in locked storage when not in use. Electronic data should be password protected and access limited to essential users only. Computer screens should be located so that personal data is hidden from general view. Photographs and video or sound recordings should not be shared without the express consent of Service Users, staff members or their legal advocates.

**Disclosure**

• Data and information should only be shared with those identified as eligible to access it. Service User data must only be shared for the purposes of ensuring individual needs are met and for the safe delivery of care. Information passed to a care worker may therefore be shared with members of the care team where they are concerned with the care and treatment of Zenith Care User. Staff must be advised of the requirement to confirm the identity and right of access of any third party seeking information about a Service User or The Agency in writing, by telephone or in person before any disclosure is made.

• Consent to disclose Service User information with family members should be obtained from Zenith Care User. There are many good reasons why informal carers should be informed and involved with the professional care of their loved one. Care should be taken, however, if a family member shows an unusual interest in their loved one's financial affairs. If family members wish to pass on their concerns or views to a member of care staff this does not constitute a breach of confidentiality by the care staff.

**Consent**

• As far as reasonably practicable, written consent to the use of personal information should be gained from each Service User or their advocate. Staff should inform Zenith Care User when gaining consent of the specific details of the information/action to be shared and with whom. This should form part of the information provided at the outset of service provision.

o If Zenith Care User lacks the mental capacity to consent to information being shared, staff may share information if it is in Zenith Care User's best interests (in accordance with the principles of the Mental Capacity Act 2005). Staff should still clearly explain to Zenith Care User the reasons for the decision to share information and accurately record these.

o Where a Service User has appointed a Lasting Power of Attorney under the Mental Capacity Act 2005 that person should be consulted where information is to be shared in someone's best interests.

o If there are any concerns in these areas you should seek advice from your supervisor.

• Access to data and records must be managed in line with legislation. Permission to access information may be sought by Service Users or their advocates in writing and access must be managed appropriately. It is good practice to involve Service Users with the collection and recording of personal data as this ensures focus on the needs and rights of each individual. This paragraph should be read in conjunction with the Access to Information Policy and Procedure.

• The use of social media should be avoided unless strict management of information is assured to protect the

rights of all Service Users and staff members. Staff must not discuss confidential information about Service Users or staff in any place where third parties might access it, such as on an outing.

• Staff must ensure that all data and information held pertains only to that individual. Care must be taken to limit recording to identify only Zenith Care User or staff member whose record it is, and not to include sensitive identifiable data about others' Care Planning files and record entries.

• Confidentiality with respect to a Service User may only be breached if:

o Where information is required by statute or court order.

o Information suggests Zenith Care User is at risk of harm to themselves or from others, or others may be at risk of harm from Zenith Care User, and where the passing on of information would be in the person's interest, or the wider public interest.

o Information, if withheld, could put others at risk; and where the passing on of information would be in the public interest.

* Where Zenith Care User may have broken the criminal law and where there is justification in the public interest to breach confidentiality, Section 115 of the Crime and Disorder Act 1998 gives a power {but not an automatic duty) to organisations to disclose information to the police 'for the prevention, detection and reduction of crime'. This applies in England and Wales and in Scotland (where the Crime and Disorder Act is amended by the Criminal Justice (Scotland) Act 2003).

• Inappropriate breaches of confidentiality by staff members will be treated as a disciplinary matter.

**Disposal of Confidential Information**

• In the event of a Service User's death or leaving Zenith Care, records should be removed from circulation and retained in secure archive storage. Care records should be kept for not less than 3 years, but it is good practice to retain records for up to 20 years to meet insurance requirements.

• When confidential information no longer needs to be stored, destruction of paper records must be by shredding to ensure no risk of third parties accessing sensitive data. Destruction of electronic records by deletion must be undertaken by means that ensure no future retrieval is possible.

|  |  |
| --- | --- |
| Signed: | \_\_\_\_\_\_\_Kechi Anyanwu\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date: | \_\_\_\_\_\_05th September 2021\_\_\_\_\_\_\_\_ |
| Policy review date: | \_\_\_\_\_20th March 2022\_\_\_\_\_\_\_\_\_\_\_ |