

<b>SHANNON COURT CARE HOME LTD.</b>	<b>Issue Date:</b> <b>April 2019</b>	<b>Reviewed July 2025</b>
	<b>Next Review: 07/28</b>	
<b>CONFIDENTIALITY POLICY</b>		

It is the policy of Shannon Court Care Home that all staff and visitors understand the principles surrounding and maintaining confidentiality, and that staff demonstrate these principles at all times.

This policy complies with the Data Protection Act 2018 and UK GDPR requirements regarding the collection, storage, processing, and sharing of personal data relating to staff, service users, and visitors.

**PROCEDURE**

**Service User Data**

All individual daily records and care plans are either stored on LogmyCare, or in individual files and then stored in filing cabinets within the unit where the service user lives. Access is limited to staff who are directly caring for the individual or any visiting professionals that require information to review the level of care that is being provided.

All electronic records are password protected and encrypted where necessary. Access is restricted to authorised personnel only, and data sharing with external parties is conducted via secure, encrypted platforms.

When service user notes are no longer required on a daily basis, the paper copies will be stored in Shannon Courts archives. Records will be stored for the stipulated period of time from their last date of entry and after this date records will be confidentially destroyed by an independent waste carrier.

A certificate will be obtained and held by Shannon Court to confirm that waste has been confidentially destroyed.

Staff will have access to service users private information on a need to know basis which translates to if a member of staff does not need to know certain information to carry out their role in relation to the care they provide to a service user, then there is no need for that staff member to be privy to the information, e.g. A nurse may need to know that a service user is allergic to penicillin but the cook and the cleaner do not need to know this information for them to provide care for the service user.

Service user's confidential information can be shared with other professionals who need to provide care for service users, however, this is on the same basis of need to know. E.g. the pharmacist may need to know that a service user has difficulty with swallowing to ensure the correct type of medication is given but a chiropodist would not need to be made aware of this information to provide appropriate care for the service user.

Confidential information related to service users or staff should never be discussed outside of the workplace.

When Shannon Court is communicating electronically with outside agencies regarding service users, only initials or the unique reference number of service user's will be used when it is

practicably possible. When communication from outside sources is sent to Shannon Court which is encrypted, Shannon Court will follow the procedures available to be able to access the information securely.

Any suspected or actual breaches of confidentiality must be reported immediately to the Registered Manager or Deputy Manager. Breaches will be investigated and may result in disciplinary action, including dismissal for gross misconduct.

Medication records on our EMAR system can only be accessed by authorised staff members. These staff members include the Manager, Clinical Lead, Nurses and Seniors for the purpose of administering medications to service users. No access can be gained without the Manager's approval. Staff members who leave Shannon Court have their access to the system removed immediately to maintain confidentiality.

### **Building Safety**

Staff members have access to all door and lift codes throughout the building. These codes must not be shared with anyone other than Shannon Court employees. This includes contractors, visiting professionals, family members and others. These codes must not be shared, as it could lead to unsupervised entry to the Home, leaving our service users vulnerable.

No photos or videos are permitted when in our building at any time, unless you have obtained written permission from the manager prior to recording. This applies to both staff members and visitors.

### **Staff Data**

Staff records will be treated with the same confidentiality, these will be stored in a filing cabinet in the Deputy Manager's office. Every staff member at the beginning of their employment will be asked to sign a confidentiality statement which is held in their personal file. This states who will be able to have access to the staff member's personal file and gives permission for them to do so. Every staff member's personal file will contain a photograph of the person.

When a staff member leaves Shannon Court, employment records are held for the stipulated period of time and then confidentially destroyed using the same procedure that is used for service user's records.

Criminal record checks will be carried out in accordance with the legislation surrounding checks and information related to outcomes from DBS will be stored confidentially in the Deputy Manager's office.

All staff and service users will be allocated a unique reference number so that in communication with outside agencies, this number can be used so that confidentiality can be maintained. A record of the unique identifiers will be stored in the Deputy Manager's office.

Any suspected or actual breaches of confidentiality must be reported immediately to the Registered Manager or Deputy Manager. Breaches will be investigated and may result in disciplinary action, including dismissal for gross misconduct.

### **CCTV**

Shannon Court has an on site CCTV system which captures any person having business with

Shannon Court and living at Shannon Court if the service users are outside the premises in an area that is covered by the CCTV cameras.

The CCTV system uses fixed and mobile cameras. There are 29 cameras placed around and inside the Home.

Staff and visitors are made aware that CCTV is in use as appropriate signage is in place.

Cameras have been positioned so they do not capture pictures of people not visiting the premises

The recorded images are stored securely and remain on the system for only 28 days so that images are retained long enough for any incident to be investigated.

The Home is aware that it has an obligation under the data protection act that it has a responsibility for ensuring that personal images are kept confidential, images can be made available to the police if required.

When information is requested by relatives/ friends either via telephone or face to face staff will only give the information to the nominated next of kin. Via telephone this information will be limited as proof of identity can not be confirmed. If the service user has capacity and requests that they do not wish for information to be given, staff will honour their wishes unless the non disclosure could cause harm to the service user or other individuals.