

# Date Protection and Confidentiality Policy and Procedure

## Date Protection and Confidentiality

This policy details the rights of Service Users in relation to confidentiality, UK GDPR, data protection and the issues that staff need to be aware of.

### 1. Policy

- 1.1** 4EVER CARE UK LIMITED recognises that we have a duty of confidentiality to our Service Users and staff. We believe that respecting an individual's right to a private life, which includes confidentiality, is important in ensuring a trusting, caring environment where both Service Users and staff are confident that information about them will be protected safely and not shared inappropriately or unnecessarily.

It is the policy of 4EVER CARE UK LIMITED that we will only share information that is in the best interest of the Service Users and with their consent. Sharing of information will be carried out in line with UK GDPR and the Data Protection and Mental Capacity Act policies and procedures at 4EVER CARE UK LIMITED.

We aim to comply with the relevant legislation and include the Caldicott principles (<https://www.gov.uk/government/publications/the-caldicott-principles>)

### 1.2 Core Principles of Confidentiality

- All staff will ensure that all Service User information remains confidential. Service Users have the right to expect that personal information held about them is not accessed, used or disclosed improperly
- The same duty of confidentiality applies to personal information about staff, with the exception of names and job titles. Information about Directors, which is published and therefore is a matter of public record, is also excepted
- All staff have the individual responsibility for ensuring that they conform to the Caldicott principles, UK GDPR, Data Protection Act (DPA) 2018 and Article 8 Human Rights Act (HRA) 1998
- Staff must not inappropriately access, misuse or share any information or allow others to do so. Staff are personally liable for deliberate or reckless breaches of UK GDPR, Data Protection Act may be liable to disciplinary action and/or prosecution
- Any personal information given or received in confidence for one purpose may not generally be used for a different purpose, or passed to anyone else without the consent of the provider of the information

### 1.3 The Position of 4EVER CARE UK LIMITED on Confidentiality

- We will share with Service Users, their families and their Care Workers, as far as the law allows, the information they want or need to know about their health, care and ongoing treatment sensitively and in a way they can understand
- Confidential information will not be used for a different purpose or passed on to anyone else without the consent of the information provider
- There may be occasions when it can be detrimental to the Service User or to another individual if this principle is strictly adhered to
- There is a recognition that breaches of confidence are often unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security. However, the consequences can be equally serious for all concerned

- 4EVER CARE UK LIMITED will ensure that personally identifiable information will always be held securely and, when used, treated with respect. This rule will apply regardless of where the information is held
  - Although the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act no longer applies to identifiable data that relate to a person once they have died, we respect that any duty of confidence established prior to death continues after a Service User has died
  - All information regarding the Service Users we support will be treated with respect and integrity
  - We will be transparent in our approach to ensure that anyone associated with 4EVER CARE UK LIMITED (whether Service User or staff or visitor) is fully aware of how, what, when, who and why we share any information about them and source their agreement before doing so
- 1.4** All relevant staff will be bound by their professional code of practice issued by their relevant licensing body, such as the General Medical Council, The Nursing and Midwifery Council and the Royal Pharmaceutical Society. Care Workers will follow the Skills for Care Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England.
- 1.5** All staff must sign a confidentiality agreement as part of their contract of employment (a template can be found within the forms section of this policy). The confidentiality agreement also extends to agency and contract workers.
- 1.6 Responsibilities - Registered Manager**
- Ensuring that systems and processes are in place for the security of records and they are reviewed to ensure that they remain fit for purpose
  - Ensuring that all staff understand this policy at the start of employment and that its importance is reiterated during supervision or team meetings
  - Ensuring that staff have received the appropriate training and are competent in their role
  - Reviewing, monitoring and auditing practice within 4EVER CARE UK LIMITED to ensure that staff remain knowledgeable
  - Acting on any breaches in confidentiality in a timely manner and notifying the appropriate bodies
  - Ensuring that confidentiality rules are never used as a barrier to sharing appropriate information and fulfilling Duty of Candour obligations
- 1.7 Responsibilities - All staff will ensure the following:**
- All information that is received is effectively protected against improper disclosure when it is received, stored, transmitted and disposed of
  - Confidential information is only accessed if it is appropriate to the job being undertaken
  - Every effort is made to ensure that Service Users understand how information about them will be used before they supply any confidential information
  - When Service Users give consent to disclosure information about them, they understand what will be disclosed, the reasons for disclosure and the likely consequence/s
  - Service Users understand when information about them is likely to be disclosed to others and that they have the opportunity to withhold their permission
  - If disclosing information outside the team, that may have personal consequences for Service User, that consent is obtained from the Service User
  - If the Service User withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:
    - They can be justified in the public interest (usually where disclosure is essential to protect the Service User or someone else from the risk of significant harm)
    - They are required by law or by order of a court

- If required to disclose confidential information, staff will only release as much information as is necessary for the purpose
- The person(s) to whom information is disclosed understands that it is given to them in confidence which they must respect
- When disclosing confidential information, staff must be prepared to explain and justify the decision. Where there are doubts, they will discuss them with
- Queries concerning this policy will be brought to the attention of
- During the induction period for new staff, they will be made aware of this policy and their individual responsibilities

## 1.8 Coronavirus

During unprecedented times, such as the coronavirus pandemic, 4EVER CARE UK LIMITED recognises that information may need to be shared quickly, or ways of working adapted. Where this is required, it will be done in line with UK GDPR, data protection requirements.

## 2. Procedure

**2.1** 4EVER CARE UK LIMITED will detail with transparency how confidentiality is managed with Service Users, employees and others at the earliest opportunity and seek their agreement, e.g. through existing systems such as recruitment and the pre-assessment process.

Staff can refer to the Fair Processing Notice Templates and the Fair Processing Notice Policy and Procedure for further information that details how information is processed within 4EVER CARE UK LIMITED.

## 2.2 Sharing Information with Other Health and Social Care Professionals

- Information sharing between partners directly involved in a Service User's care, and for the purpose of providing that care, is essential to good practice.
- Consent from the Service User for information sharing must be recorded following a discussion with the Service User or, in the absence of capacity to consent, their designated other.
  - The principles of sharing information are:
    - Only information that needs to be shared
    - Only with those who have a clear need to know
    - There is a lawful basis for sharing information

## 2.3 General Principles of Confidentiality - Staff will:

- Understand and follow the Caldicott Principles
- Be aware that the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) are not barriers to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
- Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared and will seek their agreement unless it is unsafe or inappropriate to do so
- Seek advice from your Line Manager, if they are in any doubt, without disclosing the identity of the person, where possible
- Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Staff may still share information without consent if, in their judgment, that lack of consent can be overridden in the public interest

- Consider safety and wellbeing: Staff must base information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions
- **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information shared is necessary for the purpose for which it is being shared, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely
- Staff must keep a record of any decision and the reasons for it (to include what has been shared, with whom and for what purpose), and for the decision not to share

## 2.4 Maintaining Confidentiality

- All information regarding the people we support will be treated with respect and integrity
- In general, no information may be disclosed either verbally or in writing to other persons without the Service User's consent. This includes family, friends and private carers, and other professionals
- If in doubt, you can consult your Line Manager or the Registered Manager
- Conversations relating to confidential matters affecting Service Users must not take place anywhere they may be overheard by others, i.e. in public places - such as supermarkets, public transport, open plan areas of the office, during training or group supervision where other staff not involved in the Service User's care are present
- Written records and correspondence must be kept securely at all times when not being used by a member of staff. Timesheets, rotas, etc. must not be left in an unattended vehicle
- Rotas must not contain key safe or door entry codes with Service User's name and address
- Staff must ensure their copy of the rota is confidentially destroyed. It must not be placed in household recycling
- Staff must not disclose any information that is confidential or that, if it were made public, may lead to a breakdown in the trust and confidence that the Service User and their families have in 4EVER CARE UK LIMITED
- Staff must not pass on any information or make comment to the press or other media. Media enquiries should be referred to the person responsible for handling any media enquiries

## 2.5 Safeguarding, The Care Act and Confidentiality

- Where safeguarding issues arise and in order to fully understand what has gone wrong, Safeguarding Adult Boards may ask for information to be shared. Decisions about who needs to know and what needs to be known should be taken on a case-by-case basis, within locally agreed policies and the constraints of the legal framework.
- However:
- Staff must verify the identity of the person requesting the information whilst establishing if it can be anonymised (refer to 5.8)
- Information will only be shared on a 'need to know' basis when it is in the best interests of the adult
- Confidentiality must not be confused with secrecy
- Informed consent should be obtained, but if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement
- It is inappropriate for 4EVER CARE UK LIMITED to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk

## 2.6 Rights of All Service Users

- All Service Users may view personal information we hold about them. Local and health authorities are not required to give access to information that is 'hurtful' or 'that would breach the confidentiality of another Service User'. The policy at 4EVER CARE UK LIMITED is to record information in a way that, as far as possible, avoids a need for this exclusion. If a Service User believes their right to confidentiality is either being breached or undermined, they must have access to the complaints procedure at 4EVER CARE UK LIMITED.
- Staff must refer to the Subject Access Requests Policy and Procedure for further details.

## **2.7 Rights of All Staff**

All staff may view personal information held by 4EVER CARE UK LIMITED that relates to them, by applying in writing to their Line Manager or Registered Manager, .

## **2.8 Data Security and Quality**

- Any record that contains information about an individual must remain confidential unless it is in the public domain. All records must be factual and not include the personal opinions of the person writing the records. Staff can refer to the Record Keeping Policy and Procedure for further details
- Reproduction of information relating to a Service User (e.g. photocopying documents) will only be done with the consent of the Service User
- Confidential information to be posted must be marked 'Private & Confidential, for attention of the addressee only', and sent recorded/special delivery  
As a minimum:
  - Information held within 4EVER CARE UK LIMITED will not be shown to unauthorised individuals or be left where authorised personnel may access them. All records will be kept in a lockable cabinet in a lockable office, with restricted access
  - All written records will be kept securely and only disposed of by shredding, after appropriate timescales. Staff must take care when recording personal identifiable information into personal notebooks or paper during shift handover and ensure the safekeeping and destruction of the information
  - Written information also relates to key safe numbers and Staff Rotas. Staff must be only provided with key safe numbers if they are directly providing care for the Service User and staff must follow the key safe number policy. Key safe numbers must not be recorded on Service User records for use outside the office or on rotas supplied to staff. Staff must ensure that if they record Service User information to support the delivery of care (e.g. a request to cover an unplanned absence) that the information is recorded safely and securely, and that the information is safely destroyed after use
  - Any rotas must be returned to the office for confidential disposal
  - Any employee who breaches this policy may be subject to disciplinary procedures

## **2.9 Social Media**

Staff are not permitted to discuss the people who use our services, other employees past or present, or 4EVER CARE UK LIMITED on any social networking site, as this may breach confidentiality and bring 4EVER CARE UK LIMITED into disrepute. Staff must also be aware that this applies to taking and posting photographs, videos of Service Users.

## **2.10 Mental Capacity and Confidentiality**

The Mental Capacity Act 2005 and associated "Best Interests" applies to adults without capacity, and further details about the disclosure of confidential information about a Service User lacking capacity can be found in the Mental Capacity Act Code of Practice.

## **2.11 Anonymisation and Pseudonymisation Considerations**

### **Anonymisation**

- Anonymised information (i.e. where personal information is removed and both the giver and the receiver are unable to identify the Service User) is not confidential and may be used outside of data protection legislation. However, staff should be aware that information which contains small numbers of person identifiable information may lead to identification. For this reason, all disclosure of anonymised information must be reviewed on a case-by-case basis. 4EVER CARE UK LIMITED will seek to anonymise collective data about individuals within the service.

### **Pseudonymisation**

- Pseudonymisation is the practice of removing and replacing actual data with a coded reference (a 'key'). 4EVER CARE UK LIMITED will consider this practice where the use of the data needs to relate to individual records, but also needs to retain security and privacy for that individual. There is a higher privacy risk and security risk of the key system as the data will not truly be anonymised.
- Personal data that has been pseudonymised can fall within the scope of data protection legislation, depending on how difficult it is to assign it to a particular individual. Further information can be found within the ICO Anonymisation Code of Practice (<https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>).

## **2.12 4EVER CARE UK LIMITED Confidentiality**

### **Suppliers**

- Staff must extend the principles of confidentiality when considering 4EVER CARE UK LIMITED sensitive information and the protection of any commercial data. Staff and/or external suppliers will ensure that information such as suppliers' prices, performance and costs are not disclosed to other suppliers or unauthorised persons. 4EVER CARE UK LIMITED could consider requesting that suppliers sign a confidentiality agreement in order to protect the data of 4EVER CARE UK LIMITED.
- If there are any queries about how to support commercially sensitive information, these must be discussed with your Line Manager.

### **Meetings**

- 4EVER CARE UK LIMITED has a right to have confidential meetings where information is discussed and then held securely and confidentially. Information held will be in line with the Freedom of Information Act (FOIA) 2000, the UK GDPR, and the Data Protection Act 2018.

### **Complaints and Investigations**

- Complaints and investigations are treated confidentially and remain so, unless there is a legal requirement to release information.

### **Media**

- Staff must not pass on any information, or make comment, to the press or other media. Media enquiries must be referred to the person responsible for handling any media enquiries.

## **2.13 Confidentiality Breach**

- Unauthorised access, use or disclosure may be in breach of UK GDPR, the DPA 2018, the Human Rights Act, and/or breach the policies of 4EVER CARE UK LIMITED and may lead to disciplinary action.
- Where there has been a breach in confidentiality, this will be recorded on an incident form at 4EVER CARE UK LIMITED and reported to your Line Manager.
- Significant breaches will be reported to the Registered Manager so that reporting to the relevant regulatory, professional bodies and the ICO is considered.
- Breaches will be monitored by the Registered Manager, reflected on with lessons learned and will form part of the quality assurance programme for 4EVER CARE UK LIMITED.

- Staff will refer people to the Complaints, Suggestions and Compliments Policy and Procedure at 4EVER CARE UK LIMITED.

#### **2.14 The National Cyber Security Centre**

Alongside this policy the National Cyber Security Centre has provided a useful resource centre that will assist 4EVER CARE UK LIMITED in improving and keeping up to date with Cyber Security. The Small Business Guidance is formulated under five steps:

- Step 1: Backing up your data
- Step 2: Protecting your organisation from malware
- Step 3: Keeping smartphones and tablets safe
- Step 4: Using passwords to protect your data
- Step 5: Avoiding phishing attacks

Alongside this are additional resources that are available to use. 4EVER CARE UK LIMITED will make full use of this resource tool such as the Cyber Action plan. Vital resource: <https://www.ncsc.gov.uk/collection/small-business-guide>