

# CONFIDENTIALITY POLICY

This policy applies to all staff.

## BACKGROUND

We hold all personal information under strict legal and ethical obligations of confidentiality. We must not use or disclose information that is given to us in confidence in a form that might identify a service-user (or other identifiable individual) without his or her consent. The same principle applies to staff and carer records.

There are a number of important exceptions to this rule that are described below, but we must, in most circumstances, involve service-users and others, including carers and colleagues, in decisions about use of their personal information.

Service-users have the right to access their personal files, including paper and electronic files however there are restrictions on when and how they can do this (see section 10).

## 1. INTRODUCTION

Service-users have a right to expect that our services will hold information about them in confidence. Confidentiality is central to trust between service-users and the service providers. Our handling of confidential personal information must:

- promote, support and protect the privacy, dignity and rights of our service-users
- command the support of service-users, the public, staff, students, volunteers and partner services
- comply with best practice
- conform with the law
- promote the care and welfare of service-users and the effective operation of the service.

Other considerations

- Without assurances about confidentiality, service-users may be reluctant to give information we need in order to provide high-quality services and care.
- Staff must always be able to justify decisions about information sharing or disclosure in accordance with this guidance.
- Failure to comply with this guidance and these instructions may lead to disciplinary proceedings.

## 2. LEGAL AND PROFESSIONAL BASIS

- All staff have a statutory obligation to safeguard the confidentiality of personal information. The relevant legislation includes the Data Protection Act 1998, the Human Rights Act 1998, common law and employment law. It is also central to professional codes of conduct. All staff must be aware that any breach of confidentiality may be a matter for disciplinary action or provide grounds for complaint or private legal action against them by the individual(s) concerned.
- If you have fully informed the person about the range of uses you may make of information they give you, you do not need to seek their specific consent each time you pass on information for a particular purpose.
- You must control access to personal information on a strict need-to-know

basis when you are sharing information with other agencies. Where you are dealing with agencies not involved directly in the case, for example, where you are asking an organisation to search a database, you should ensure that you give them no more than the minimum information required.

If someone states that they do not want to have their personal information shared, you must respect their wish unless there are exceptional circumstances. You must make sure that you explain fully the consequences of withholding information for care or planning.

### 3. General principles

- In all cases, you must restrict the amount and type of information to what is necessary in the particular circumstances.
- You must not use information supplied for one purpose for another purpose.
- You must consider whether the information can be shared in anonymised form.

## 4. CONSENT BY THE SERVICE-USER

- You must explain to the service-user that a refusal to give information or allow it to be shared may make it more difficult, and sometimes impossible, to provide appropriate advice or services.
- At the beginning of any period of contact, including for assessment or service, you should obtain the service-user's consent to share information within Normal Limits (see below) by asking them to fill out a form of authority. You must explain the nature and likelihood of the normal limits to the service-user and any other person giving information.
- You are asking the service-user to give ongoing consent to information sharing, so that you do not have to seek consent on every occasion that information sharing is necessary. You must make sure that the service-user has the opportunity to identify and comment on agencies or individuals that are likely to share information at the beginning of this process.
- The service-user can change the terms of their consent or withdraw it completely at any time. You must discuss the implications of any change or withdrawal with them.
- If a request for information sharing does not come within the usual Normal Limits but is not Exceptional, you must get the service-user's specific consent to share their information.
- You must also advise the service-user of the Exceptional Circumstances (see S.7 below) in which you may need to share information without consent or, indeed, prior knowledge. You should try to advise the service-user before the information is shared unless that would risk harm to another person or impede the investigation of serious crime.

## 5. INFORMATION FROM CHILDREN

- Children and young people of all ages have the same rights to confidentiality as adults.
- Even where the child may not have capacity to consent to or refuse disclosure (see below), they have the right to talk in confidence with any other person.
- If the child does not understand the consequences of confidentiality, you must

explain to the child that some information may need to be shared with the people with parental responsibility for the child or with other people, especially if there are exceptional circumstances.

- If you decide not to share the information with the parents, you must record the reason.
- Children who are deemed capable of understanding the implications of medical treatment and, therefore, capable of consenting to it, have the right to be consulted and to be treated by medical practitioners in confidence.
- If the child is deemed to be capable of understanding the consequences of confidentiality, their consent is required for disclosure or access to records. In relation to data protection and access to records, a child of 12 or over is normally assumed to have sufficient understanding. You may only override a child's consent or refusal where there are issues relating to the child's capacity (for example, where the child has some degree of learning disability).
- Where you are dealing with a capable child, you must ensure that any decision you make about sharing or disclosing information without their consent, or in spite of a refusal, satisfies the Exceptional Circumstances outlined in S. 7 below.
- If the child is not considered capable of understanding the consequences, then their parents or guardians must consent to disclosure, or request access.

### **6. NORMAL LIMITS OF INFORMATION SHARING/DISCLOSURE**

To carry out assessments and to provide effective services, you will usually have to seek information from, and share information with, other agencies or individuals who hold relevant information. This may include:

- staff, directly involved in the services-user's case and care
- senior staff and trustees who have management functions or when investigating and handling of complaints
- other colleagues, including service support staff (receptionists, finance staff, administrators and assistants), who will need or will have access to the information as part of their work
- other agencies and professional staff, for example, health, education and housing, to enable the right provision to be made
- other agencies or carers undertaking work with the same service-users in partnership or on behalf of local authorities - this would include foster carers and residential staff, for example.

The normal limits of information sharing will be explained to the service users and agreed with them on the authority form.

### **7. EXCEPTIONAL CIRCUMSTANCES IN WHICH INFORMATION MAY BE DISCLOSED WITHOUT CONSENT**

Disclosure of personal information without consent may be justified where failure to do so may expose the service-user or others to risk of serious harm. You should always make every effort to gain consent but the health and safety of the individual has primacy over the right to confidentiality. Exceptional circumstances include:

- child protection: staff should adhere to the Policy on Protection from Abuse.
- protecting vulnerable adults

- life threatening or dangerous situations, for example, where a young person:
  - shows signs of physical, emotional or sexual damage
  - is at risk of significant harm or threatening suicide
  - is threatening to kill or severely harm another person
- the prevention, detection or prosecution of crime
- risk assessment of sex offenders.
- people who are missing and individuals who may be in need of protection
- prevention or reduction of risk to personal or public health.

There is a legal obligation to provide information in the following circumstances:

- requirement by a court/police.
- disclosure to Appointees.

## **8. PROCEDURE FOR DISCLOSURE OR SHARING OF INFORMATION TO OTHER PEOPLE OUTSIDE OF THE NORMAL LIMITS**

Before sharing the information outside the normal limits, you should, where necessary, obtain advice from your line manager. The form of authority will outline the levels of disclosure agreed with the service user.

You must consider:

- whether to seek the consent of the service-user or the person who has given the information
- how or if the service-user or person who has given the information will be advised that information has been disclosed
- what you will do if consent is refused
- whether advance warning of the disclosure may present risks, for example:
  - to the service-user or others, or
  - by hindering police inquiries
- whether to seek the views of investigating police officers, if the disclosure is related to an investigation of crime.

## **9. KEEPING INFORMATION SAFE**

- You must make sure that you protect personal information about service-users (and others, including carers and colleagues) against improper disclosure at all times.
- Many improper disclosures are unintentional. You must not discuss identifiable service-users in circumstances that do not come within the normal limits or exceptional circumstances described earlier.
- When discussing service-users, you must ensure that you cannot be overheard by anyone not bound by the same requirements of confidentiality towards that service-user.
- You must not leave material containing personal data, either on paper or on computer screen, where it can be seen by other service-users, unauthorised staff or other visitors to the office or unit.

- You must keep all portable records containing personal data in recognised filing and storage places. This storage should be locked at times when access is not directly controlled or supervised.
- You should switch off computers with access to client information, or put them into a password-protected mode, when you are not working on them.
- From time to time, you may need to keep material with personal identifiable data in places other than the service-user's file. You must keep all such material under the same secure conditions as other service-users' files.

## **10. SERVICE USERS ACCESS TO FILES**

Service users can have access to their files however there are certain restrictions to protect staff and other service users.

- Service users can have access to all their case notes, support plans and other documents.
  - Staff can refuse to allow service users to access information if access to that information would prejudice the accuracy of a risk assessment. This means that all or part of a risk assessment may be kept confidential from the service user, This information will be held in their file in an envelope marked confidential.
  - Staff should try to ensure that the service users has a member of staff or other person present when they read their file to provide emotional support or explain aspects of information recorded.
- Original documents should not be held on file but should be kept by the service users and a copy kept on file. Originals should always be returned to clients when their case is closed.**