

Key Worker Skills

Factsheet



Confidentiality

- Make sure your computer screen cannot be seen by service users, visitors or unauthorised staff
- Do not share your password with anyone, not even other members of staff
- Do not hold confidential conversations in public or in inappropriate places where they can be overheard, such as in corridors, open plan offices or on buses

Confidentiality & service users

When accessing the service for the first time service users and their advocates must always be informed that you cannot guarantee absolute confidentiality in all circumstances. You are legally required to share information in the following circumstances

- Safeguarding children
- Safeguarding vulnerable adults
- Preventing an act of terrorism

Data protection examples

- Remember not to store service user's personal information on memory sticks or CDs etc
- Electronic records if you are sending service users information to an e-mail address outside of your organisation, make sure that the service users identity is protected e.g. use initials or an ID number. Do not refer to the service user by their full name
- When working in an office, make sure when you leave your desk that service users' personal information or other sensitive information is filed away in secure cabinets
- When leaving your desk ensure personal information is filed away and ensure that all confidential information is not left out overnight

Record keeping

- The police, solicitors or service users themselves may request personal data, therefore it is vital that the procedure for requesting information is followed.
- When recording information do not write information relating to a third party in service user's notes. If there is any information relating to a third party, make sure this is removed when handing over information to the service user.
- When recording information remember not to write anything down as factual if it is based on personal opinion e.g. use words like "he/ she seemed, he/ she appeared" not "he/ she was" unless we know this to be true

Definitions

Managing Risk

The process by which the organization/service identifies risks, assesses their relative importance, determines appropriate risk controls and ensures appropriate and timely action is taken.

Identifying Risk

The information gathering process where a service user's risks are established (through examining referral information and through speaking with the service user and key agencies working with them).

Analysing Risk

An assessment of the impact of the service user's risks and their affect on the service user, their environment and those they come into contact with.

Controlling Risk

The management of risk through a risk management plan, in conjunction with other agencies.

Key Worker Skills

Factsheet



Information sharing

In order to share a service user's personal information, we must have an information sharing agreement in place with key agencies we work with. Information sharing agreements must specify what information will be shared and under what circumstances. Service users and/ or their advocates must also sign a confidentiality waiver and sign to say they consent to treatment.

N.B. information sharing agreements need to be reviewed every three months in line with good practice guidelines. All information sharing agreements must be signed by the service user and key worker.

Impacts of not following principles correctly?

The individual

- The wrong care plan or risk assessment may follow them
- Mental and physical health may deteriorate
- Family/ personal relationships may break down
- May place in danger to self or others
- Could lead to confrontation, anger, mistrust, upset etc
- Puts in a complaint

The team

- Demoralised if unsure of "how" to
- Affects quality of care, outcomes not achieved
- Service user disengages
- May place self, team, service user or other service users/ third parties in danger
- Other agencies may receive wrong information and therefore SU could be denied a service
- If consequences/ implications of not doing a care plan are severe, staff may leave their job, be suspended or dismissed

The organisation

- Reputation is damaged
- Name in disrepute
- Loss of clients
- Loss of service
- Reduces quality
- Claims due to inadequate management of care

A key worker should....*

- Ensure the regular delivery and review of the service user's care plan and risk assessment
- Set goals and time frames which are revised as appropriate
- Builds a therapeutic relationship with the service user
- Work with other agencies (within a multi disciplinary team) to co-ordinate the service user's support
- Protect the service user and other vulnerable adults and children from harm
- Inform their manager as soon as possible if they feel the service user is overstepping a professional boundary

A key worker should not...*

- Act outside of their role and their competence
- Correspond with a service user on a social networking website
- Enter into a situation with a service user which could potentially bring financial or personal gain
- Breach confidentiality guidelines
- Not share personal information (such as personal contact details, information about your family and friends) with the service user

*Not exhaustive list