Consent and Confidentiality Common Principles

Information for Professionals

CONSENT:

Agreement made voluntarily by an individual with mental and legal competence (i.e. capacity to understand the implications of information sharing).

BEST PRACTICE:

Explicit Consent:
This is written consent to carry out a specific action and is the type of consent needed when sharing any information. An individual must be asked for specific consent for a specific action for it to be considered "explicit".

Informed Consent:
"Informed consent" is consent given by an individual only after having received and understood a detailed explanation of the proposed action. Informed consent is usually demonstrated by signing a consent form.

Implied Consent:
When a service user is aware of the potential for sharing information and his/her right to refuse and makes no objection, this could be construed as 'implied consent', however, this is not valid under the Data Protection Act 1998.

Consent at Earliest Time:
Consent should be gained from an individual at the first instance, or as soon as practicably possible thereafter.

Capacity to give consent:
You may feel that a person does not have the capacity to give informed consent. If so, then an authorised member of staff needs to confirm that the person does not have capacity to make a decision about sharing information accordingly. Wherever possible, the issue should be discussed with relatives and carers. You should record decisions about an individual's capacity and your subsequent action.

Recording Consent:
Consent forms – for children; for young people and for parents/carers - should be used. This should then be stored in the individual's file, and a copy given to the individual. Use of the consent form should be regarded as best practice. Where the consent form is not used (i.e. where some other form of written consent is given) then this must be clearly recorded and dated. In every case, practitioners must clearly record any restrictions or limitations that the individual has placed on information sharing, such as the type of information which can be shared or the agencies with which it can be shared.

Reviewing Consent:
Consent to the sharing of information should not be viewed as a 'one-off'. An individual may decide to change or withdraw consent previously given. Throughout the individual's involvement with services, it is best practice to review consent with each new case or circumstances. Consent should be reviewed regularly, for instance on an annual basis. A record should be kept of the date

consent was given, the due date for consent to expire and, if appropriate, the date that consent was changed or withdrawn.

Disclosure without Consent:
If consent is refused, professionals can still legitimately share information in limited circumstances. These include safeguarding the vital interests of the individual; protecting the health, morals, rights and freedoms of any person; or to prevent or detect crime. In practice, a decision to share information without consent will most often be made in child protection situations, or to prevent a serious criminal act. Professionals should refer to the 'Disclosing Information without Consent' form and associated guidance (The Moray Council).

Using Professional Judgement:
Information must only be shared on a "need to know" basis. Information sharing is justified on this basis if it is clearly in the best interests of the service user. When requesting information, professionals should be able to state the purpose of the request and must demonstrate that sharing information is in the best interests of the service user.

Security of Information:
Secure means that all reasonable steps have been taken to prevent the information being passed to or accessed by someone that does not have a right to it. Only individuals who need to have access to the information should have access to it, and even then they should only have access to information that they need to see. For electronic information this may mean introducing access controls.