Principles of information sharing

Effective information sharing is key to the delivery of PREVENT, so that partners are able to take appropriately informed action.

Key Principles

Partners may consider sharing personal information with each other for PREVENT purposes, subject to a case by case basis assessment which considers whether the informed consent of the individual can be obtained and the proposed sharing being necessary, proportionate and lawful.

Any sharing of personal or sensitive personal data should be considered carefully, particularly where the consent of the individual is not to be obtained. The legal framework within which public sector data sharing takes place is often complex, although there is a significant amount of guidance already available.

Necessary and Proportionate

The overriding principles are necessity and proportionality. It should be confirmed by those holding information that to conduct the work in question it is necessary to share the information they hold. Only the information required to have the desired outcome should be shared, and only to those partners necessary. Key to determining the necessity and proportionality of sharing information will be the professional judgment of the risks to an individual or the public.

Consideration should also be given to whether discussion of a case is possible with anonymised information, for example, referring to “the adult” without the need to give the individual’s name, address or any other information which might identify them.

Each case should be judged on its own merits, and the following questions should be considered when sharing information:

- what information you are intending to pass;
- to whom you are intending to pass the information;
- why you are intending to pass the information (i.e. with what expected outcome);
- the legal basis on which the information is to be passed

Consent

The default should be to consider seeking the consent of the individual to share information. There will, of course, be circumstances in which seeking the consent of the individual will not be desirable or possible, because it will prejudice delivery of the intended outcome, and there may be gateways or exemptions which permit sharing to take place without consent. If you cannot seek or obtain consent, or consent is refused, you cannot share personal information without satisfying one of the gateway or exemption conditions. Compliance with the Data Protection Act and Human Rights Act are significantly simplified by having the subject’s consent. The Information Commissioner has indicated that consent should be informed and

unambiguous, particularly in the case of sensitive personal information. If consent is sought, the individual should understand how their information will be used, and for what purpose.

Power to Share

The sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the Data Protection Act, the Human Rights Act and the common law duty of confidentiality. Some statutes confer an express power to share information for a particular purpose (such as section 115 of the Crime and Disorder Act 1998). More often, however, it will be possible to imply a power to share information because it is necessary for the fulfilment of an organisation's statutory functions. The power to share information arises only as a consequence of an organisation having the power to carry out an action which is dependent on the sharing of information.

Having established a power to share information, it should be confirmed that there are no bars to sharing information, either because of a duty of confidentiality or because of the right to privacy enshrined in Article 8 of the European Convention on Human Rights.

Finally, it will also be necessary to ensure compliance with the Data Protection Act, either by meeting the processing conditions in Schedules 2 and 3, or by relying on one of the exemptions (such as section 29 for the prevention of crime). Further details of the overarching legislation and some potentially relevant gateways are set out below.

Where non-public bodies (such as community organisations) are involved in delivery of PREVENT work, you may need to pass personal and sensitive information to them and your approach to information sharing should be the same – i.e. that it is necessary, proportionate and lawful. In engaging with non-public bodies to the extent of providing personal information, it is good practice to ensure that they are aware of their own responsibilities under the Data Protection Act.

Vetting

Sharing information to prevent violent extremism should not be impeded by issues surrounding vetting. If there is a requirement for the sharing of material above restricted level the need for vetting need not be a barrier. Practitioners should consider ways to share the information which needs to be shared to enable partners to provide the necessary response. Consideration about whether it is appropriate for an individual to be vetted should be decided at a local level and on a case-by-case basis, depending on requirement and necessity.