**Data Protection – information sharing guidance**

**Introduction**

The Organisation holds huge amounts of personal information about people. Our use of this information is regulated by the Data Protection Act. The DPA is that it does not forbid any information sharing. It does not contain rules. However, it does provide conditions that must be met before sharing can go ahead. The Act should never be used as an excuse not to share, because the Act does not automatically forbid anything.

On the other hand, you should follow the Data Protection principles even it might seem less efficient or slower than simply ignoring the act and sharing when you need to. There will be a way to share information legally. The earlier you think about the implications of DP before you share, the easier it will be to follow them. Considering DP at the last minute, when you have already made the decisions about how to proceed, will make things more difficult.

How to ensure that you are sharing information correctly.

The key points are:

* Ensure that people know that their information will be shared
* Ensure that either the Organisation’s notification covers the sharing, or that an amendment will be made to it
* Ensure that the Organisation has the power to share the information

**Obtaining information**

When information is obtained from people, it is vital that they know how that information is to be used and shared. It is part of the Organisation’s responsibilities under DP to ensure that people are informed about sharing. Therefore, if they are told about sharing when the initial contact is made, it should not be necessary to tell them later on.

**New processes and services**

Any new procedure or service must be examined to ensure If consent is necessary for the disclosure, that consent will in all normal circumstances be obtained at the time when the individual gives their information to the Organisation. If consent is not necessary because of a legal obligation, people should still be informed. Consideration of the legal reasons for sharing information should be part of the process of developing the new service or process. It must not be done at the end, when all the decisions about how the service will work have already been made.

**Making Data anonymous**

If the data being shared can be made anonymous, then the demands of Data Protection do not apply. Therefore, if it is practical to make data anonymous before it is shared, it should be.

When information is shared, only the minimum necessary will be exchanged – existing sources will be edited or altered before being transferred to ensure that extra information is not included.

**Understanding of the law**

All departments will take steps to ensure that they understand the legal framework in which they are working in order to ensure that they can share information when requested, and where they need to do so to provide an efficient service.

**Checking the identity of requester / validity of the request**

Where information is requested by an outside body, Organisation employees will take all reasonable steps to verify the identity of the person making the request. Personal information will not be supplied without some identity checks taking place. Whenever possible, requests for information should be obtained in writing to make clear what is required.

Where an outside body claim the right to access information about people held by the Organisation, the legal basis of that right must be checked. This can be done by the department, or in consultation with the Data Protection Officer. Organisation staff must not supply information to an outside organisation without receiving some form of documentary evidence proving their right to demand the information.

**Security of information transfer**

Information will only be shared in secure circumstances.

Adequate measures will be taken when sending information to outside organisations to ensure that the information will only be seen by the appropriate people. Information should only normally be disclosed to a specific named individual.

**Contracts and agreements**

Contracts and agreements which include the transfer of personal information will contain appropriate protections to ensure that information is only used for the purposes of the agreed purposes, and not used or disclosed for any other reason without further consultation.

Contracts, agreements and protocols controlling the transfer or exchange of information will include a phase of consultation to ensure adequate protections for personal data. In these circumstances, agreements written by other organisations will not be signed without being reviewed for their adherence to good practice on Data Protection and confidentiality.

**Sharing agreements**

Where information is to be shared on a regular basis between the Organisation and an outside organisation, the department in question will develop an information-sharing agreement which sets out the circumstances in which information will be exchanged, and the protections provided to individuals.

Information–sharing agreements will be made available to the public and published as widely as necessary.

**Crime prevention and detection**

The Organisation will endeavour to assist all relevant law enforcement organisations by disclosing information where appropriate to assist in the prevention or detection of crime, or the assessment and collection of tax. Where this involves disclosing information about named individuals, this will be done in accordance with the Data Protection Act. Organisation employees will always ask relevant authorities to establish their right to request information, and satisfy themselves that such a right is valid, before sharing the information.

**Confidentiality**

Information which is given with an expectation of confidence can only subsequently be disclosed in exceptional circumstances. Employees will be aware of their responsibilities when accepting information in confidence, and not disclose it to anyone else without the permission of individuals.

If the information is about a crime or other serious wrong-doing, employees should always inform the supplier of information that they have a duty to report any criminal activity to the proper authorities if they become aware of it.

**Individual’s access to their own information**

Information about individuals will always be disclosed to them following the receipt of a valid subject access request under the Data Protection Act. The Organisation will endeavour to supply information under the subject access provisions as soon as possible, and well within the 40 day time limit. The Organisation will ensure that when a subject access request is received, information about third parties will only be disclosed with their consent, unless there is an overwhelming.

**Unauthorised disclosure**

It is a criminal offence to knowingly or recklessly disclose personal information without the consent of the individual, or another legal obligation. Staff who knowingly disclose or misuse information for any reason which does not have lawful authority may be subject to disciplinary action.