South Cambridgeshire District Council **Data Protection**

How does Data Protection affect you?

If you handle or have access to personal data which is both of a sensitive and non-sensitive nature about the general public or SCDC employees then this act applies to you. The Data Protection Act enables individuals to know what personal information is held about them and that only specifically authorised people have access to that information.

What is personal data?

Personal data is anything which identifies an individual, this is either on it's own or referenced to other information which is kept by the District Council. Personal data can be classed as Name, Address, Telephone Number, Sex etc. The Act recognizes that some types of personal data are more sensitive than others. There are extra rules for processing data about your ethnic origin, religious beliefs, trade union membership, sexuality etc.

What must I do?

You must make sure that information regarding personal data on computers and paper based systems are managed properly in accordance with the 8 principles of the Act. You need to inform the Data Protection Officer that you hold such information in a system, or have introduced a new system.

What has South Cambridgeshire District Council done?

The Council has:

- Appointed a Data Protection Officer (see last page)
- Notified the Information Commissioner (a government appointed 'watchdog') of the type of information we hold on individuals.
- Set up a process (SAR – Subject Access Request) which

allows individuals to find out what the Council holds on them in terms of their Personal Data.

- Undertaken a Data Protection Audit of all personal data that held on individuals in all parts of the Council, in order to check compliance with the Act.
- Issued guidance on appropriate wording to be used in all data collection forms, including a statement about data protection. This is available on the ***Intranet*** under document 'Data Protection statement for forms'.
- Improved our ICT Security Policy and Disaster Recovery Plans.
- Built Data Protection into the Induction course & Induction handbook for new staff.
- Re-formed a Data Protection Act working group that meets every three months and is led by the Data Protection Officer.
- Introduced a complaints procedure for data protection and subject access requests.
- Introduced a procedure for gaining consent in the use of images of people (general public & employees of South Cambs).
- Each department to have elected representative who will monitor the application of the Data Protection Act within their department.

Remember that….

New ICT systems and changes in Council services mean we must all continue to be vigilant about security of information and other aspects of Data Protection. The last page of this leaflet gives a checklist of items that you may wish to consider as a team or on a personal basis. **All employees are responsible for ensuring that their own collection and processing of personal data and sensitive personal data are in accordance with these procedures.**

The Eight Principles of the Act

These eight principles state that personal data will be:

1. Processed both fairly and legally.
2. Processed for limited purposes and in an appropriate way.
3. Relevant, adequate and not excessive for the purpose it is intended.
4. Kept accurate and up to date.
5. Retained for as long as necessary and no longer.
6. Processed in accordance with the rights of the individual.
7. Kept securely.
8. Only transferred to countries that have suitable data controls.

Here are the eight principles in a bit more detail:

First Principle -Personal data must be processed both fairly and legally.

Processing means collecting, storing, retrieving or organising data. This can only happen if the individual concerned (data subject) gives their permission, or the processing is necessary for legal or contractual reasons. To be processed fairly, the data subject should know who is processing data about them, and why. Individuals must not be deceived or misled about why the data is needed. To be processed legally the data must not lead to any form of discrimination or other law breaking. If personal data is going to be disclosed to a third party then this must be declared.
Forms for collecting personal data must include a Data Protection Act statement, see 'Data Protection statement for forms'.

Second Principle - Personal data must only be processed for limited purposes and in an appropriate way

For those who are collecting data, you must only do so for a valid reason and inform the individual of the reason. Data collected for one service cannot be used for any other unrelated purpose. For example, names and addresses held for a particular purpose must not be given to a mail order company without permission.

Third Principle - Data must be relevant, adequate and not excessive for the purpose.

Only data really necessary for the purpose stated should be collected. Information which may be used at a later date should not be collected. This information should be collected when it is needed.

Fourth Principle - Personal data must be accurate and up to date.

Anyone collecting and using information should take all reasonable steps to check it for accuracy, whether it originates from the individual concerned or some other source. Information liable to change over time should be monitored to ensure it is kept up to date, if it continues to be processed. Personal comments about an individual can be recorded if they are relevant, objective and kept up to date. Please remember that the individual concerned can ask to see what has been said about them.

Fifth Principle - Personal data processed for any purpose should be kept no longer than is necessary to fulfill that purpose.

Out of date or redundant information should be got destroyed in a confidential manner on a regular basis. For example, application forms from unsuccessful job applicants should be destroyed after a few months (see Record Retention Guidelines).

Sixth Principle - Data must be processed in accordance with the rights of the individual

These rights include the right of access by the individual to information held about them, as well as the right to prevent processing likely to cause damage or distress to themselves or anyone else. There are exceptions to these rights. For example, individuals do not have such strong rights in cases of crime detection or taxation assessment.

Seventh Principle - Data must be kept securely

Controls may be technical (e.g. built into computer systems) or organisational (e.g. management structures and physical security in the work-place). When you have finished work make sure that you lock away all files, letters etc, which would have personal details. Also you must lock (ctrl+alt+del) your computer when you are away from your desk and shut your computer down when you leave work at night.

Eighth Principal - Data can only be transferred to countries that have suitable data controls.

Not all non-European or European countries have data protection legislation, however there is limited transfer of data with other countries here at South Cambs District Council.

Consent for taking images for use in printed publications or on the intranet/internet

This is a new procedure in terms of the use of pictures of people for printed publications and intranet/internet. This procedure can be found on the intranet as well as in the Media Guidelines Protocol.

Important! - Consent must be actively sort from the subject of your image, consent cannot be inferred from a failure to respond. If an individual fails to indicate that he/she does not consent this must not be taken as an indication that he/she does consent to the processing data.

Subject Access Review (SAR)

Any individual has the right to have a search conducted of databases, paper files etc to determine what personal data is held. We have 40 days to comply with the SAR and the response to the individual will include:

- a description of the personal data.
- why the data is held.
- who else the data might have been given to.
- a copy of the data.
- an explanation of any technical terms or abbreviations.
- any information about the original source of the data.

You may be asked by the Data Protection Officer to provide information regarding an individual as part of a SAR.

Retention of Records

It is crucial that all employees retain any communications they have with the general public. Individuals have the right to access any interactions they have had with the council. In terms of the retention of records please refer to the Records Retention Guidelines.

Checklist of Data Protection Actions

Do you/your section*:*

Comply with the 8 principles of the Data Protection Act?

In particular, do you:

- Tell individuals why you are collecting information on them?
- Get permission of the individuals to transfer that information to other organisations, if that is what you do?
- Keep all personal data/information in a secure manner?
- Have procedures to keep information up to date and accurate?
- Dispose of information no longer needed promptly and securely?
- Consider the Data Protection implications of new or amended services?

- Have you a Data Protection Representative in your section?

Do's and Do Not's

Do's

- Get consent from the individual before you do anything with their personal data.
- Take care when giving out personal data, unless you have checked the individuals identification you can't be certain of their identity.
- Inform the individuals what you intend to do with their personal data.
- Check that you really need to record their personal data.
- Make sure the data is kept secure, if data is in paper form please lock them away in a filing cabinet and if in electronic form please make sure that they are password protected.
- Remember that paper files as well as computerised data will be subject to the Data Protection Act 1998.
- Audit your manual files as soon as possible – they may be accessed by individuals.
- Register your personal data stores with the Data Protection Officer.
- Dispose of data when it is no longer required using the correct procedure – paper based by the appropriate confidential waste disposal and electronic documents deleting them from the system.

Do Not's

- Give out information to anyone about an individual without their prior consent.
- Write down anything you wouldn't want someone to see, i.e. inflammatory comments about members of the public.
- Post personal data on web pages without the individual's consent – not even departmental web sites.

- Use the personal data for another purpose other than that which it was collected for.
- Assume the District Council has blanket cover for your purposes – it hasn't.
- Assume it is someone else's responsibility to register the data stores.

Help/Advice/Training

The Council's Data Protection Officer is Daniel Horrex (Information Management Officer – ICT division). Daniel is happy to provide information and advice on any aspect of Data Protection, including training for individuals or sections, and to deal direct with the public on specific issues. He can also supply the forms by which individuals can request information on what data the Council holds on them, although these forms and associated guidance are also available at the main Reception at South Cambridgeshire Hall and on the Intranet & Internet.

Data Protection as an employee

In terms of the Data Protection Act, the Council's duties apply equally to us all as members of staff. Your rights include (for example) the opportunity to see your personal file held by your Chief Officer. You have a right for your image to not be processed in any way which you haven't consented to. For further details see 'Data Protection Act and the use of images' or in the Media Guidelines.