



## **POLICY STATEMENT ON DATA PROTECTION**

### **1.0 Policy Statement**

- 1.1. The Council of the City & District of St Albans is fully committed to compliance of the Data Protection Act 1998. The Council will therefore follow procedures that aim to ensure that all employees, councillors, contractors, consultants, agents and partners who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties & responsibilities under the Act.
- 1.2. To carry out our work and meet legal responsibilities the Council has to collect and use information about the people with whom it works. These may include members of the public, clients, customers, suppliers and employees.
- 1.3. The Council is also be required by law to collect and use information in order to comply with the requirements of the Central Government.
- 1.4. The Council considers that the lawful and correct treatment of personal information is most important to our operations and in maintaining confidence between the Council and customers and those with whom we carry out business.

### **2.0 Background**

- 2.1 All staff and councillors are required to protect personal information from unauthorised disclosure. There are legal penalties for unauthorised disclosure of personal information.
- 2.2 In accordance with the requirements of the Data Protection Act, the council is registered with the Information Commissioner for activities which involve processing personal information. There are currently 2 registrations, one for general council functions (Z5700229), and one for electoral registration (Z763263X). Each registration has to be renewed annually.

- 2.3 Personal data is held in many forms – computer records – databases, spreadsheets and documents; on imaging systems; on laptop computers; in paper files; microfiche; CD's, floppy disks and memory sticks; PDA's and mobile devices etc.
- 2.4 Particular care must be taken with personal data stored on devices which are used away from the office environment, or at the homes of councillors or home workers.
- 2.5 Members of the public have a legal right to request access to or copies of their personal data held by the Council. A request for personal data should be made in writing and is called a Data Subject Access Request.
- 2.6 Additional rights for members of the public under the Act include – preventing processing of data likely to cause damage or distress; preventing use of personal data for marketing; correcting or deleting information that is not accurate; complaining to the Information Commissioner.

### **3.0 Responsibilities**

- 3.1 Staff are expected to carry out their jobs in a way that supports the Councils' responsibilities under the Data Protection Act. In particular, that means protecting personal data from unauthorised access and complying with data subjects' rights under the Act. It also means taking special care of files or electronic records containing personal data.
- 3.2 Staff are expected to be aware of the principles of data protection as set out in Appendix 1 and only to use the personal information they process for the legitimate purposes for which it was collected.
- 3.3 Managers must ensure that their area of operation complies with the Act and their use of personal data is covered by the registration with the Information Commissioner. Managers must also ensure their staff, including any temporary, agency staff and work experience placements, are aware of relevant policies and procedures. Any new activities that involve processing personal data must be notified to the Data Protection Officer so that the appropriate registration can be updated with the Information Commissioner.
- 3.4 Managers need also to develop and apply procedures for deletion of information, disposal of redundant records containing personal data and archiving historical records. The Council will develop corporate policies and procedures for records management and retention.

- 3.5 Any staff involved with processing personal data away from the office environment must be approved for such work in accordance with the home and remote working policy.
- 3.6 Staff must not informally pass on personal data to other organisations. Guidance for compliance in relation to data sharing has been issued by the Information Commissioner (see Appendix).
- 3.7 Managers and staff need to appreciate the risks of communicating personal information by e-mail or messaging systems, and publishing personal data on the internet, because of limitations of security of those systems.
- 3.8 Care must be taken when using personal information such as names and addresses from a database for promotional or marketing purposes. The consent of data subjects is required for these purposes.
- 3.9 Care must be taken when disposing of records and files containing personal information. Paper records that are no longer required should be disposed of by sacks for shredding of confidential material. Electronic records containing personal data must be reviewed regularly to ensure compliance with Data Protection principles.

#### **4.0 How the Council deals with requests under the Data Protection Act.**

- 4.1 A formal request for information under the Data Protection Act must be in writing and sent to the Data Protection Officer at the Council. Requests may also be made by e-mail or fax. A verbal request will not be accepted.
- 4.2 The request will be acknowledged upon receipt, and any clarification of the request (if it is not completely clear what is being asked for) must be sought promptly. A person who asks to see all personal information about them held by the Council, may reasonably be asked to say in which department or service area the information could be held.
- 4.3 Details of the request – date of receipt, summary of information requested, deadline for response – will be recorded on a corporate spreadsheet or database for monitoring purposes.
- 4.4 A request received by a department may be dealt with directly by appropriate staff in departments, and details recorded on the corporate spreadsheet/database. The Data Protection Officer is available to advise.
- 4.5 Requests received by the Data Protection Officer will be forwarded promptly to departmental information officers who deal with Freedom of

Information Act requests, managers or heads of service, as appropriate, with confirmation of the deadline for dealing with the request.

- 4.6 The Council will charge the statutory fee of £10 in respect of a formal request under the Act. Requests must be dealt with within 40 calendar days.
- 4.7 This procedure will not be applied to routine interviews, discussions and correspondence with customers which may require confirmation of their personal data and are part of the regular business of Council departments. Staff who are regularly communicating with customers on this basis have still to observe the principles of data protection and satisfy themselves as to the identity of any customer requesting access to personal.

**CONTACT DETAILS:**

**Post:** Data Protection Officer, St Albans City & District Council, District Council Offices, St Peter's Street, St Albans, Herts AL1 3JE

**Telephone:** 01727 866100

**E-mail:** [foi@stalbans.gov.uk](mailto:foi@stalbans.gov.uk)

## **5.0 Data Protection Act information – Appendices**

**Appendix 1** – Data Protection Principles

**Appendix 2** – Data Protection Act Glossary

**Appendix 3** – Exceptions to the data subject access provisions

**Appendix 4** – Data Protection Do's and Dont's

**Appendix 5** – Guidance from the websites of the Information Commissioner and Department of Constitutional Affairs

**Appendix 6** – Information Commissioners Advice - Providing Information to a Third Party

**Appendix 7** - Information Commissioners Advice – Data sharing between local authority departments

**Appendix 8** - Information Commissioners Advice – Council Tax – Secondary use of personal information held for collection and administration

## **APPENDIX 1 Data Protection Act Principles**

The Data Protection Act sets out eight principles, which restrict the reasons for which personal data may be obtained and specifies how it can be used.

- Personal data must be fairly and lawfully processed
- Personal data shall be processed only for one or more specified and lawful purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
- Personal data shall be accurate and when necessary, kept up to date.
- Personal data shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For a more detailed explanation of the Data Protection Act principles see also:

[www.informationcommissioner.gov.uk/cms/DocumentUploads/Data Protection Act 1998 Legal Guidance.pdf](http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%201998%20Legal%20Guidance.pdf)

## APPENDIX 2 Data Protection Act Glossary

Data	Information which is processed by equipment operating automatically stored in a structured filing system or is an 'accessible' record (housing and social services records).
Data Subject	Individual who is the subject of personal data.
Data Controller	Individual who determines the purposes for which and the manner in which personal data is processed by the Council.
Data Processor	Any person or organisation who processes the information on behalf of the Authority but is not responsible for determining purposes and manner of processing.
Disclosure/Recipient	Other parties to whom the personal data can be disclosed
Information Commissioner	The national regulator for Data Protection and Freedom of Information legislation.
Sensitive Personal Data	Personal data about racial or ethnic origin, political opinions, religion, trade union membership, physical or mental health, sexual life, criminal offences or proceedings. More stringent requirements apply to the disclosure of sensitive personal data.
Subject Access Request	A request for personal information
Third Party	A person other than the data subject who is identified during the subject access request
Personal Data	Information that relates to a living, identifiable individual and affects that individual's privacy, whether in his personal or family life, business or professional capacity.

Concept of  
Privacy

Account should be taken into whether or not the information in question is capable of having an adverse impact on the individual.

A recent court case (Durant –v- Financial Services Authority) considered the meaning of ‘personal data’. The conclusions of this case were:

Where a person’s name appears in information, the name will only be ‘personal data’ where its inclusion affects their privacy. It is more likely that an individual’s name will be ‘personal data’ where the name appears together with other information about the named individual such as address, finances, telephone number or information regarding hobbies.

Providing the information in question can be linked to an identifiable individual the following are examples of personal data:

- Information about the medical history of an individual;
- Salary details;
- Tax liabilities;
- Bank statement;
- Information about spending preferences.

These types of information may be contrasted with the following examples of information, which will not normally be personal data:

- Reference to a person’s name where the name is not associated with any other personal information;
- Incidental mention in the minutes of a business meeting of an individual’s attendance at that meeting in an official capacity; or
- Where an individual’s name appears on a document or e-mail indicating only that it has been sent or copied to that particular individual, the content of that document or e-mail does not amount to personal data about the individual unless there is other information about the individual within it.

Further detail is provided on the Information Commissioner’s website at <http://www.informationcommissioner.gov.uk>

### **Appendix 3 – Exceptions to disclosure of personal data**

The council is exempt from the duty to disclose personal data it holds in certain circumstances.

- Where disclosure of the data will involve the disclosure of data relating to another data subject (third party). In this situation, the consent in writing of the other data subject will also be required.
- Where a previous request has been made which is identical or similar and no reasonable time has elapsed since that request
- If the information is already publicly available
- Information about proceedings subject to legal professional privilege
- Management forecasts
- Information about ongoing negotiations
- If disclosure would involve a disproportionate effort when compared to the benefit that will be enjoyed by the data subject in receiving that information.
- In the cases of health, education and social services records, where it could result in serious harm to the physical or mental condition of the data subject or another person.
- Where it would not be in the interests of prevention or detection of crime, apprehension or prosecution of offenders, assessment or collection of any tax or duty.
- Where it would not be in the interests of national security.

## Appendix 4 – Data Protection Do's and Don't's

- Do treat personal data with the greatest care
  - Do check identities before disclosing personal information
  - Do secure all personal data and dispose of confidential waste by shredding
  - Do ensure that no-one else, especially members of the public or contractors, can read other peoples' information on your PC screen. Remember there may be contractors in the office outside of office hours.
  - Do discuss concerns about personal data with your colleagues or supervisor
  - Do reassure customers and others we do business with, that we take very seriously the protection of personal information
- 
- Don't look up information on systems about colleagues, friends, relations, neighbours etc unless for legitimate work purposes.
  - Don't talk about personal information you deal with outside of work
  - Don't leave machines logged on while you are away from them even for a short time and particularly if personal information is displayed on the screen
  - Don't leave files containing personal information where they could be seen by people who are not allowed to see them.
  - Don't tell anyone your computer password
- 
- Only use personal data for the purpose it was collected. If you want or need to collect additional data discuss with the Data Protection Officer as the Data Protection Act registration may need to be amended
  - Only disclose personal information to those people with a need and a right to know and if in doubt contact the Data Protection Officer

## Appendix 5

### Guidance from the Information Commissioners Website & Department of Constitutional Affairs

The following Guidance documents have been published by the Information Commissioner to help those in the public sector comply with the Data Protection Act. Go to: <http://www.informationcommissioner.gov.uk/eventual.aspx?id=438>

#### Legal Guidance

CCTV

Child Support Agency: Maintenance Assessment, Uses and Disclosure

Council Tax: Secondary Use of Personal Information

Electoral Register: Use in Light of the Robertson Case

Notification / Registration FAQ

Schools: Exam Results Disclosure to the Media

Subject Access and Third Party Information

Subject Access to Health Records

Health Data: Use and Disclosure

Inland Revenue: Disclosures under the Taxes Management Act

Local Authorities: Disclosures to Elected Members

Local Authorities: Elected Members Advice

Local Authorities: Data Sharing

Planning Applications: Sale of Information to Local Traders (England and Wales)

Promotion of a Political Party

Registration Officers: Right to Inspect Local Authority Records

Vehicle Keepers Information: Implications on Use and Disclosures

Violent Warning Markers: Use in the Public Sector

Website FAQ

The Department for Constitutional Affairs has recently published the first instalment of a 'toolkit' which will help practitioners in the public sector work through some of the data sharing difficulties encountered by numerous public bodies. You can view this document at the following web site:

<http://www.dca.gov.uk/foi/sharing/toolkit/index.htm>

The Department for Constitutional Affairs has now published the response document to the consultation paper 'For your information: how can the public sector provide people with information on, and build confidence in, the way it handles their personal details?'. You may view the document at the following web address:

<http://www.dca.gov.uk/consult/datasharing/datashareresp.htm>

## Appendix 6

### Information Commissioners Advice

#### Providing Personal Account Information to a Third Party

##### Aim of this guidance

To help you decide whether or not you should be giving information to third parties calling on behalf of an account holder and what to say if you decide not to. This guidance would be a useful training aid for any organisation that commonly deals with personal information or that regularly faces enquiries from the general public.

##### Recommended good practice

- We know that it is not easy to judge when you can give out information and when you cannot.
- Common sense should make you cautious about releasing details of someone's account, not just the need to comply with the Data Protection Act. The Data Protection Act is here to ensure that personal information is handled fairly and securely.
- You must therefore have appropriate safeguards in place to ensure that, if you do decide to reveal account information, you are sure that the person you are speaking to is either your customer or someone acting on their behalf.

##### **For example:**

Request some form of evidence that the account holder has given their authority.

Set up a password on the account as a security measure (this may be an option for customers where someone regularly calls on their behalf, e.g. their spouse.)

- Think about whether or not you actually need to give any personal information. If not, it may be possible to speak to the caller.

##### **For example:**

Someone reporting a problem with another's phone line would not require a telecommunications company to disclose information (although if the company explained that it had been cut off for non-payment this would involve disclosure.)

- You have good reason to be careful about accepting instructions from someone other than the account holder where this will result in charges being incurred even if no personal information will be released. However, this is a matter of contractual obligations and not data protection.

### Saying no

If it is not appropriate to reveal account details to a third party, explain why you are not willing to give them any information. Something along the lines of the example below should help them to understand why you cannot deal with them.

**We have to be careful with our customers' information because there are attempts to trick us into giving it to someone who is not the customer and who is not acting on that customer's behalf.**

Remember that there may be occasions when it is reasonable to reveal some limited information about an account to someone other than the account holder.

### Good versus Bad Practice

Example	☞ Good Practice	☹ Bad Practice
<p><b>Someone calls on behalf of their elderly mother to check whether there is a valid gas maintenance contract that would cover an emergency call out and can quote details from her most recent bill.</b></p>	<p>You are confident that the caller is acting on their mother's behalf and you provide this information, it is hard to imagine why somebody would want this unless they wished to help the account holder <i>or</i></p> <p>You are not confident that the caller is really calling on their mother's behalf so are not comfortable speaking with them. You explain this rather than blaming the DPA</p>	<p>You are suspicious and refuse to release the information saying that the DPA prevents you from doing so.</p>
<p><b>Someone calls requesting details of an elderly relative's bank account. They have no account details and can offer no proof that they have been authorised to call on that person's behalf.</b></p>	<p>You are suspicious and refuse to release the information until they can provide some evidence that they have permission to act on behalf of that person. Rather than simply citing the DPA, you tell them that you need to be certain of the identity of any callers and of their authority to act for the account holder in order to avoid giving details to unauthorised people.</p>	<p>You provide the details anyhow (this is probably a breach of the DPA)</p>

**Appendix 7**  
**Information Commissioners Advice**  
**Data sharing between different departments**

The Data Protection Act 1998 came into force on 1 March 2000. It regulates the holding and processing of personal data, that is information relating to living individuals, which is held either on computer or in some cases in manual form. The Act gives legally enforceable rights of individuals (data subjects) and places obligations on those legal persons who control the manner and the purpose of the processing of personal data (data controllers). Data controllers must notify the Commissioner of the details of their processing. These details are published by the Commissioner in the register of notifications.

Data controllers must also comply with eight data protection principles which together form a framework for the proper handling of personal data. The Information Commissioner's office regularly receives enquiries about the circumstances in which personal data held by one department may be used by another department within the same local authority. This Advice Sheet explains the impact of the Data Protection Act 1998 on such further uses of personal data.

**Compliance with the first Data Protection Principle**

The first Data Protection Principle states *"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless - a) at least one of the conditions in Schedule 2 is met, and b) in the case of sensitive data, at least one of the conditions in Schedule 3 is also met."*

Thus this Principle has two elements; firstly that there is a legitimate basis for the processing and, secondly, that the information is processed fairly and lawfully.

**Schedules 2 and 3**

In order to process data legitimately, data users must be able to satisfy at least one of the conditions set out in Schedule 2 and, in the case of sensitive personal data, at least one of the conditions set out in Schedule 3 of the Act. 'Sensitive' data are those relating to ethnic origin, political or religious beliefs, trade union membership, physical or mental health, sexual life and criminal offences.

So far as local authorities are concerned Schedule 2.5(d) will usually be relevant in that most of the processing carried out is necessary *"for the exercise of any other functions of a public nature exercised in the public interest by any person."* Schedule 3 has a similar condition at 7(1)(b) which refers to processing necessary *"for the exercise of any functions conferred on any person by or under an enactment ..."*

For further information about the possible conditions for the processing of personal data, see *The Data Protection Act 1998 – An Introduction*.

### **Fair processing**

The interpretation of the First Principle in the Data Protection Act 1998 states that in order for the data to be processed fairly, when individuals (data subjects) provide information about themselves they must be told the identity of the data controller and the purposes for which their data are to be processed. They should also be provided with *“any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair”*. In simple terms this means that individuals should be made aware of any ‘non-obvious’ purposes for which the information about them may be used or disclosed. This can normally be achieved by the inclusion of a notification on forms and other documents explaining any non-obvious uses and disclosures of personal data.

### **Lawful processing**

No statutory interpretation is contained in the Act as to the meaning of the requirement to process personal data ‘lawfully’. In the absence of this the advice given by the Commissioner is that a data user who obtains information by unlawful means or processes information without any justification in law will breach the requirements of the Principle.

For public bodies such as local authorities this means that that if personal data are processed for purposes which are prohibited by statute or which are *ultra vires* then that processing will automatically breach the First Data Protection Principle. Similarly, if personal data are processed in breach of an obligation of confidence (which would be unlawful) then that processing would also breach the First Data Protection Principle.

The issue for a local authority is, therefore, whether it has the powers to process personal data obtained for one statutory purpose for another purpose, or whether it is prevented from doing so by virtue of an obligation of confidence or any statutory prohibition on processing (including disclosure). These are not fundamentally data protection questions and local authorities must take their own legal advice as to their powers and as to statutory restrictions on uses or disclosures of data.

The Information Commissioner is not able to advise local authorities on the general law although clearly there will be occasions when she may decide to seek her own legal advice. This is only likely to occur in the context of prospective enforcement action.

### **Compliance with the second Data Protection Principle**

Even when a local authority is able to comply with the terms of the first Data Protection Principle in respect of a further use of personal data the second Data Protection Principle should also be considered. This states *“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be*

*further processed in a manner incompatible with that purpose or those purposes.”*

### **Enforcement action by the Information Commissioner**

Although the Commissioner may serve an enforcement notice on any data controller she considers to have contravened or be contravening any of the Data Protection Principles she has discretion as to whether to serve these notices or not. In making that decision she will take into account the effect of the breach of the Principle on any data subjects.

We appreciate that this Advice Sheet does not provide any clear cut answers. This is because the issue of lawfulness is rooted not in the Data Protection Act but in other statute to which local authorities are subject. As an additional point it may be worth noting that as a publicly available document the Electoral Register may always be used as a source of name and address information. (Please see separate Advice Sheet on the Electoral Register).

### **Information Commissioner**

Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF Telephone:01625 545 700 Facsimile: 01625 524510  
e-mail: [mail@dataprotection.gov.uk](mailto:mail@dataprotection.gov.uk) Website: [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)

## **Appendix 8**

### **Information Commissioners Advice: Council tax – secondary use of information held for collection and administration**

#### **Introduction**

1. The Council Tax was introduced in 1992. Since that date the (now) Information Commissioner has received a large number of enquiries and complaints about secondary uses and disclosures of personal data held by local authorities for the purpose of the administration and collection of Council Tax. The most frequently asked questions are listed in the Annex. In effect the Commissioner is asked to advise on the extent to which it is possible for local authorities to make use of Council Tax data as a general information resource.

2. The Commissioner's functions relate to data protection and freedom of information. His office does not generally advise on other areas of law except in relatively general terms or where the general law and the data protection advice are inextricably linked. Therefore, the Commissioner's response to questions about Council Tax had been to advise local authorities to obtain their own legal advice as to the extent of their powers under the Local Government Finance Act 1992 (LGFA) and the associated Regulations.

3. However in view of the volume and variety of requests received for advice in this area and the relationship of those questions to issues of lawfulness under the first data protection principle, the Commissioner took counsel's opinion from a leading public law chambers and in May 1999 produced data protection guidance on the secondary uses of Council Tax data.

4. This advice note updates this guidance, taking into account the coming into force of the Data Protection Act 1998 in March 2000 (which does not materially alter the position) and also amending the Commissioner's understanding of paragraph 17 of Schedule 2 of the LGFA.

#### **Legal Advice given to the Commissioner**

5. The advice given to the Commissioner is as follows:  
Local authorities are creatures of statute and, as such, must have specific statutory authority to use or disclose information acquired by virtue of their powers to charge and administer Council Taxes for any purpose.

The scheme under which Council Tax is administered is set out in the LGFA and the Council Tax (Administration and Enforcement) Regulations 1992 ("the Regulations").

A Billing Authority (i.e. local authority) may make use of other information in its possession, except that held in its capacity as a police authority, together with information supplied by listing officers, precepting authorities, CCROs,

EROs, the Commissioner of Births Deaths and Marriages, or the Commissioner General for England and Wales, and other authorities, for Council Tax purposes. However, any information so obtained may only be used or disclosed for Council Tax purposes, unless specific statutory authority exists that allows secondary disclosure or purposes.

- There is no power in the LGFA or the Regulations to make disclosures of personal data held for Council Tax purposes for other purposes. Paragraph 17 of schedule 2 of the LGFA allows for regulations to be made for the supply of relevant information to any person who requests it for another purpose, but personal data is specifically excluded.

6. Since no other uses and disclosures are permitted, the processing of personal data for any such other purposes (or to effect other disclosures) would thus be ultra vires.

7. The Commissioner also received advice regarding the application of Section 111 of the Local Government Act 1972 to possible uses of data held for Council Tax purposes. This provides that:

“a local authority shall have power to do any thing ... which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions.”

8. It has been suggested that this provision would sanction the use of data held for Council Tax purposes for some secondary purposes, notwithstanding the fact that the LGFA and the Regulations are silent on the matter. The Commissioner is advised, however, that this is an incorrect interpretation and that this Section does not allow the exercise of powers derived from one statute for another statutory function. In particular it would not allow personal data held for Council Tax purposes to be used as a resource for other local authority purposes, even given the consent of the Council Tax payer.

9. Section 111 may, however, allow billing authorities, when advising Council Tax payers of how the local authority's budget has been allocated, to promote other Council services and to inform them of benefits and other schemes of which they may wish to take advantage.

10. In summary, the Commissioner's response to enquiries about possible secondary uses of Council Tax data is that the only permitted uses and disclosures of data are those specified in the LGFA or the Regulations, or in other statutes regulating different Local Authority functions.

## **Lawful Processing of Personal Data**

11. The first data protection principle requires that:

Personal data shall be processed fairly and lawfully...

12. Supported by the Data Protection Tribunal, the Commissioner has taken the view that the lawful processing element of this principle will be breached if there is no lawful basis for the processing of personal data or if the effect any processing is to breach a legal obligation<sup>3</sup>. For public bodies such as local authorities a key question in considering compliance with the principle is whether or not they have the power, or vires, to carry out processing. Any processing which is itself ultra vires, or is carried out for a purpose which is itself ultra vires, will necessarily breach the first data protection principle by virtue of the fact that it is unlawful.

## **The Commissioner's Enforcement Policy**

13. Breaches of the data protection principles are not criminal offences. However, where he considers that there has been a contravention of one or more of the principles the Commissioner does have the power to serve enforcement notices specifying steps to be taken to rectify the effect of the contravention and to prevent further contraventions taking place.

14. Before taking enforcement action the Commissioner must consider all the relevant circumstances, which would include any consent given by the Council Tax payer to a secondary use of the data and whether there had been any damage or distress caused to data subjects. The Commissioner is not aware of any allegations of widespread or significant areas of complaint about, or abuses of, Council Tax data by local authorities. In view of that, he does not intend to follow this advice by a compliance investigation of authorities' uses of Council Tax data. However this does not mean that he will not take enforcement action in this area, for example following a complaint from a data subject.

## **Conclusion**

15. The Commissioner recognises that the restrictive nature of the advice which he has received and of the difficulties which this may cause Councils. The Commissioner also recognises that the effect of this advice may run counter to the encouragement given to public bodies in the Modernising Government White Paper to share and make more effective use of information which they hold. He does, however, draw attention to the commitment in the White Paper to:

“provide a proper and lawful basis for data sharing where this is desirable, for example in the interest of improved service or fraud reduction consistent with our commitment to protect privacy.”

16. The Commissioner would therefore advise local authorities which wish to use personal data held for Council Tax purposes for a secondary purpose to make their representations for a change in the law to the government through the usual channels.

17. While the Commissioner's compliance staff will attempt to answer any practical questions which arise from this advice and which are not covered by the Annex, they will be unable to enter into more general discussion concerning the legal opinion received by the Commissioner which forms the basis of this advice. If authorities wish to make further legal points or raise other points for consideration, they are asked to do so in writing to the Commissioner's Legal Department.

## Annex

### Frequently Asked Questions

Q: Can a local authority make commercial use of Council Tax data, for instance by renting names and addresses of Council Tax payers to third parties for marketing purposes?

A: No. There is no power in the LGFA or the Regulations to allow disclosures of personal data held for Council Tax purposes for purposes other than Council Tax administration.

Q: Could a local authority conduct a mail shot on behalf of a commercial organisation (and thus avoid making a disclosure of personal data)?

A: No. Such a use of personal data is not provided for by the LGFA or Regulations, and could not be considered as being reasonably incidental to the other functions of the local authority.

Q: Can a local authority disclose (or confirm) the addresses of Council Tax payers to third parties such as public utilities for debt tracing purposes?

A: No. There is no power in the LGFA or the Regulations to allow disclosures of personal data held for Council Tax purposes for purposes other than Council Tax administration.

Q: Can an electoral registration officer make use of Council Tax data in compiling the electoral roll?

A: Yes. Regulations made under the Representation of the People Act 2000 give registration officers the power to inspect records held by local authorities for the purposes of "registration duties". Therefore the disclosure to the electoral registration officer is permitted under statute and therefore is not unlawful.

Q: Can a local authority make use of its Council Tax database in tracing its own debtors?

A: Yes, if the debts in question relate to the Council Tax. However, the LGFA and Regulations do not give authority for the use of personal data held for Council tax purposes for the tracing or collection of other debts.

Q: Can a local authority enclose a survey about its services with its Council Tax canvass forms?

A: Yes. Such an activity would be considered to be reasonably incidental to the authority's general functions and would be permitted by Section 111 of the Local Government Act 1972.

Q: Can a local authority use Council Tax mailings to promote other council services?

A: Yes. Section 111 of the Local Government Act 1972 would allow the authority to promote its services at the same time as it advised tax payers of how revenues raised by the tax had been spent.

