Data Protection policy

Introduction

1. The Data Protection Act 1998 (the Act) governs the management of personal data, and hence protects privacy, in organisations like City of York. It has four main aspects:

   - **Rights** of "data subjects" (living individuals, such as York citizens and the council's clients, customers and staff)
   - **Obligations** on "data controllers" (those processing personal data, such as the council)
   - **Exceptions** to those rights and obligations
   - A **regulation and enforcement** regime including the office of Information Commissioner, and public "notification" to him by data controllers which process personal data.

2. This policy describes how the Act will be put into effect by City of York. It uses the Act's terms and definitions. It does not restate the Act's features. The Council must have mechanisms to ensure it can meet its obligations and these are described here. Where there is discretion, the criteria to be applied in reaching a decision are described here.

Data Protection Policy

3. City of York recognises personal privacy not as a bureaucratic burden, but a way to enter individual relationships through procedures that are consistent, professional and responsive. The maintenance of individual privacy is a basic, although largely invisible, aspect of public service. The Act and this policy provide a vocabulary to express the council's view of its relationships with citizens and customers.

4. Respect for subjects' rights, particularly fair processing, puts the citizen in control. Where people can be offered a choice about how their data may be used, or re-used, it will be made as easy as possible for them to exercise that choice.

5. This policy applies to the following data controllers:

   - City of York Council
   - City of York Electoral Registration Officer
   - City of York Superintendent Registrar

- each of the councillors of the City of York.

Each of these will notify to the Information Commissioner their processing of personal data as required under s 17 of the Act.

Directors

6. It is the responsibility of **directors** to ensure that all the rights and obligations of the Act are observed. This will include

   - providing a service privacy statement for each of their services. Preparation for this will include identifying legal provision to ensure processing is lawful and fulfils the relevant conditions[1], and identifying exemptions where they are relied on by a service in carrying out its functions

   - ensuring each of the data protection principles is given due consideration for every transaction of personal data. Guidance on each is given below.

   - ensuring that the Notification in respect of their services is complete

7. In addition the Director of Resources will provide an **advice and audit** service to assist directors, and will report to the Executive member annually on the operation of this policy. The ITT department will provide security and back-up facilities and advice on management of electronic data. The Human Resources service will arrange for training to be provided within the corporate training programme in response to needs identified by Directors or through the advice and audit function.

8. Directors will devise procedures and security measures to ensure that the Act and this policy are observed.

General

9. All personal data will be **prepared and recorded** as if in the expectation that it will be disclosed to the data subject, even if it is expected to be exempt, and even if it is in an unstructured manual file. Recorded personal data will therefore be factual and objective; opinions will be professional and defensible, and all expressed in temperate language.

[1] As required by the first data protection principle (see annex). In general item 5b of schedule II and item 7b of schedule III will be relied on in preference to consent

10. The separate identities of **children** (and vulnerable adults) will be respected. Parents (and carers) must be shown to be acting in their interests, and not their own, before they can exercise the child's rights or insist on the council's obligations. However where parents' and carers have rights (or the council has obligations) under other legislation of course they will be respected[2].

11. Requests made by data subjects for **access to their own data** will usually be managed within the relevant department as part of its regular service. However (as with FoI requests) where exemptions may be claimed, or where requests plainly cover more than one service, the Subject Access Request Procedure will apply. Such requests will be tracked through the FoI tracking routine. The director of the department receiving the request is responsible for managing it but will consider the advice of the Director Resources before claiming exemptions.

12. **No fee** will be charged unless the request is for education records to which a higher fee may be applicable; if so the higher fee is at the discretion of the Director of Learning Culture & Children's Services.

13. HR procedures provide for access by each employee to his or her **Human Resources file**. Staff or personnel files will be treated as the personal data of staff members whether or not they fall within the definitions of the Act. Information will therefore usually be accessible to staff members on request unless exempt. Where items or files are held in more than one location (for instance split between physical and electronic files, or between HR and line management) a request will be taken to refer to **all material** unless its scope is restricted by agreement with the employee. But where an employee believes data is held in unstructured manual files he or she must indicate, reasonably accurately, where the search should be made.

14. **Partnerships:** Data sharing with partners is simply another form of processing and is therefore governed by this policy in all respects. Regular data sharing with other organisations will be governed by agreements ("protocols") made with them. Further guidance on the features of a good agreement is given below. Agreements serve to show data subjects the rules that will ensure that their rights are observed, and may fulfil the function of a service privacy statement. The absence of a protocol will not prevent *ad hoc* data sharing which must nevertheless be described in the service privacy statement.

15. Breaches of this policy will be considered by the Council to constitute a **disciplinary offence**. Each case will be considered on its merits after

---

[2] eg parents have a right to reports on a child's progress at school up to the age of 16 under the Education Reform Act 1988

due investigation in accordance with the Council's disciplinary procedure. However, without prejudice to due process, a breach leaving the Council liable under the Act will be considered to constitute an act of gross misconduct.

Application of the Policy

Relationship to other policies

16. The council's Information Management Charter describes how the Act and the Freedom of Information Act 2000 define the relationship with customers, citizens and communities. There is a Subject Access Request Procedure to guide officers when data subjects exercise their rights. All are underpinned by the records management policies which ensure that data and information can be located and retrieved and rights and obligations observed. There is a diagram showing how these policies relate to each other at Annex A.

17. Human Resources policy includes a right of access by any staff member to his or her personal data in their HR file, and this Policy confirms that right.

18. This policy promotes respect for, and maintenance of, privacy in general. But from time to time legitimate breaches of privacy may be necessary (eg for the prevention of crime or to protect the rights of others). They will be governed by particular policies and procedures, including:

- the Electronic Communications Policy: employees' private emails and telephone calls and internet use can only have a limited expectation of privacy
- Fraud Response Plan: investigation of alleged fraud or corruption by employees, councillors or others
- Internal Audit Terms of Reference: imposes a professional duty of confidentiality over personal data included in routine Internal Audit samples
- IT staff handbook: imposes a separate duty of confidentiality, and data security, on IT staff handling (or discovering) personal data while administering computer systems.

Collection of personal data

19. Personal data must be collected fairly, and to achieve this each service will provide or make available a privacy statement describing

- how it will use the data
- to whom it might be passed both internally and externally
- mandatory and voluntary restrictions on its use

- anything else that a data subject might not reasonably know or be able to deduce.

20. If personal data is **collected from outside** the council the subject is to be informed that this has happened. There is no need to include details that are obvious – perhaps if the data subject has already been told what to expect, or has requested it – but there should be enough information to allow an interested person to find out everything he or she might need to know. People must not be misled by commission or omission.

21. **Exemptions** may apply in some services and where they are routinely relied on should be noted in the Service Plan. Crime prevention is an example. The legal basis for processing personal data (and indeed for providing the service) should also be noted in the Service Plan. These requirements fulfil the first data protection principle.

22. Where **consent** is relied on, there must be a mechanism to record it. If this is not practical, or is stated in the privacy statement, there must at least be a mechanism to allow it to be withdrawn, and a record made, and for processing to be stopped. Where some other condition is relied on it must similarly be recorded.

Processing personal data

23. First DP Principle: application of the above section will ensure that the First DP Principle is applied.

24. The Second DP Principle restricts the **re-use of personal data**. The threshold is low[3]; the secondary use must not be inconsistent with the first. However departments will ensure there are no specific limitations on re-use and will observe them if identified. The Fair processing principle means that the data subjects should be informed of the secondary use as soon as possible. Re-use or secondary use mean a purpose not described in the Privacy Statement or Service Plan so they must be added asap and IMO informed so that the Notification can be brought up to date.

25. Data collection for **Council Tax** purposes is the subject of specific Information Commissioner advice. If another purposes arises the advice of the Information Management Officer or other qualified person is to be considered. However the council has specific legal advice that it is proper to re-use the council tax database to populate (and refresh) the Customer Relationship Management system (CRM). Further use from this source is subject to the second DP principle as set out above.

[3] see DCA guidance on information sharing (Nov 2003)

26. Use of personal data for **marketing** purposes will (exceptionally) rely on consent and be subject to an opt-in system where possible and an opt-out system otherwise.

27. The Fifth DP Principle requiring **deletion of personal data** once its purpose has been fulfilled will be incorporated into each department's records retention and deletion schedules (as required under departmental records management policies).

28. The Seventh DP principle requires suitable **security measures**. For electronic data the Information Systems Security Policy[4] will apply. The application and configuration of those measures, training, and supervision of them, rests with departments; as does that for other files and documents including manual files, audio and video recordings and any other forms of personal data.

29. Transmission of personal data to other organisations must be suitably secure, having regard to the sensitivity of the data and the number of records involved. Where both are high, tighter control is required to ensure there is no loss of control over the privacy of the data[5].

Right of access: definitions of personal data and of relevant filing systems

30. The Durant judgement of November 2003 defined these more closely with implications for the application of the Act[6]. Under this policy the rights and obligations of the Act will be applied to the **paper components of employee personal files** as well as the electronic components. Therefore directors will ensure that all eight data protection principles are applied to them and that, in order to permit access by the subject, all staff-related material is stored systematically so as to facilitate quick and efficient retrieval.

---

[4] still only available in draft (June 2008)

[5] the loss by HMRC of disks containing personal data of 25 m child benefits claimants in November 2007 has given this a high public profile. Note that the data itself is not lost; the disks are, and with them control over disclosure and re-use of the data.

[6] Mere mention of a person is not necessarily his personal data; to be so it must impinge on a person's privacy in some way; information must have the person as its focus. A judgement is to be made of where, on a "continuum of relevance and proximity" to him or her, the information lies. A manual file must do more than have a person's name on the front – it must provide access to specific items of information as easily as a computerised system. A collection of documents in date order is probably not sufficiently structured.

31. **References to a person must be found** before a decision can be made as to whether or not it amounts to personal data. Therefore all electronic references must be located (perhaps using search facilities or software) and a decision made. It is possible that narrowly-focussed personal data exists within a document even if the principal content of the document is not the person's data, and documents must be redacted or edited accordingly.

32. It is a matter of fact whether data is a person's personal data, and whether access to it can be required by that person. Directors will consider the **advice of the Director of Resources**, or professional legal advice, before withholding data grounds of being not personal.

33. However the following **need not be searched** for apparently personal data in response to a request from a data subject, unless he or she indicates that personal data will be found there[7] or they are filed by reference to the person:

- paper diaries (but electronic diaries must)
- "blue books" or note pads
- documents carrying hand-written comments.
- Binders, folders or wallets of paper documents not structured by reference to people.

but note that printed copies in the above may be of electronic documents which must themselves be located and searched for personal data.

Directors

34. This policy is intended to guide the directors of City of York Council in recognising and responding to the Act. However in most cases decisions and responsibilities will be delegated to service managers and the **Director of Resources will delegate** to the Information Management Officer.

35. The **EASY@York** project, which incorporates the Council's response to e-government obligations, will change the way that customers and citizens do business with the Council and make requests for information. It is likely to mean that information is reused for all council services, with customers informed accordingly.

[7] under S 7 (9A) of DPA which deals with unstructured personal data

Other public authorities, third parties, and contractors

36. Where information is routinely disclosed or shared with other data controllers then **information sharing protocols** should be prepared and agreed. Their purpose is to agree in advance why and how the sharing can be made consistent with each body's data protection policy, and to save making individual decisions for each transaction. Protocols should seek to avoid repeating the text of the Act, or its guidance or codes, or the policies of each party; rather they should concentrate on explaining to a data subject that his or her rights are being properly protected, and to an employee why it is right to disclose (or refuse to). A protocol is like a visa for an item of information; it shows that the necessary consideration has already been given for information falling within the categories defined by the protocol.

37. **Data processing contracts** must ensure that the council is properly indemnified in respect of breaches of a data subject's rights by the contractor. Standard contract terms are available from the IMO whose advice should be considered before entering such a contract.

38. **Partnerships:** Where a third party holds or processes the data of a person who is also a council data subject the service manager must consider who the data controller is and whether a data processor relationship exists. IMO can advise where there is doubt. Where the council is the data controller this policy is applicable; where another body is an information sharing protocol should be considered.

Exemptions: **Crime Prevention**

39. When personal data is requested by another data controller (eg the police) or by another council service under S29[8], almost any of the rights and obligations of the Act might be suspended. A director (or service manager with delegated responsibility) must be satisfied that

- refusal would prejudice the investigation, and
- the inrtusion into privacy is proportionate to the crime

before making the disclosure. This may require further explanation by the body or service making the request and a form may help where this happens regularly.

[8] for the purpose pf the prevention or detection of crime, or the apprehension or prosecution of offenders, or the collection of tax

Complaints

40. Complaints will be handled through standard Council procedures. The address, and that of the Information Commissioner, is to be provided to anyone whose request has not been met in full, as a standard paragraph.

Management

41. This policy is to be promoted within departments **by each director** and responsibility for compliance lies with them. To assist directors in this the Director of Resources will make available advice and guidance, training, and an audit service to test compliance and report to directors with recommendations for improvement if necessary.

42. To promote this policy the **Director of Resources** will maintain organisational connections between directors, service managers, and his own information management functions as defined in the Information Management Charter. Directors will make available officers with suitable seniority, training and experience to provide liaison and help ensure compliance with this policy in their department.

43. This policy and the Procedure will be applied by **service managers** as an integral part of their service delivery. An understanding of these policies is one of the competencies required of them.

44. The Director of Resources will **report** on the application and progress of this policy annually to the members' Information Management Champion.

Bibliography

Data Protection Act 1998, OPSI http://www.opsi.gov.uk/acts/acts1998/80029--d.htm

Freedom of Information Act 2000, HMSO
http://www.legislation.hmso.gov.uk/acts/acts2000/20000036.htm

Code Of Practice on The Management of Records by Public Authorities Lord Chancellor's Department, 20 November 2002 (the "S46 code")
www.dca.gov.uk/foi/codemanrec.htm

Public Sector Data Sharing: guidance on the law Dept for Constitutional Affairs November 2003 http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm

Relevant City of York policies:

Information Management Charter
Records Management corporate and departmental policies
Electronic communications policy
Information systems security policy
Document retention policy
Human Resources manual
Equalities policies