NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

POLICY AND RESOURCES CABINET BOARD

18 February 2016

Joint Report of the Head of Legal Services - D. Michael
and
Head of ICT and Procurement - S. John

Matter for Information

Wards Affected: All Wards

Report Title: Data Protection Briefing

Purpose of the Report

1. To brief Members in relation to Data Protection issues.

Executive Summary

2. In accordance with the recommendations of the Information Commissioner arising out of a report on the processes of the Local Authority, the following actions have been undertaken:-

- The preparation of training materials for all staff
- The development of instructions relating to "Subject Access Requests" from members of the public

- The further development of procedures to consider self-reporting to the Information Commissioner of losses and/or unauthorised releases of personal information.

Background

3. The Data Protection Act 1998 (DPA) imposes certain obligations on the Council as a Data Controller as to how it handles the personal information which it holds about individuals, and how it deals with requests from individuals who want to gain access to any personal information which the Council holds in relation to them, (which are known as Subject Access Requests).

4. The Council is registered as a Data Controller with the Information Commissioner and has to have appropriate policies and procedures in place to protect personal data.

5. The Council holds a large amount of personal data in both electronic and paper form. This includes personal data of varying sensitivity. Inevitably, due to the functions of the Local Authority, some of that information is of an extremely sensitive nature (e.g. Social Services data).

6. The 8 Data Protection Principles enshrined in the DPA are set out below:-

- 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 personal data, at least one of the conditions in Schedule 3 is also met.

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, 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.

7. Officers are considering the position on data protection issues in the development of the Council's Risk Management Policy and Risk Registers. Public Authorities have been heavily penalised by the Information Commissioner in the past in respect of unauthorised data releases and loss of data. The County Borough is not one of those public authorities but, bearing in mind the nature of the information which we hold, the many ways in which that information is handled, interaction with other public bodies and the inherent risk of human error data protection and data security issues will continue to be of concern.

8. The Council's Head of Legal Services is the Data Protection Officer and the Head of Information Technology and Procurement is the Senior Information Risk Officer. In the Information Commissioner's Audit of the Authority, training and awareness of staff was identified as a weakness. Whereas new entrants to the County Borough are given information appropriate to employees on the duties which apply in the handling of personal data, this information was regarded as insufficient by the Information Commissioner. There was a fundamental difficulty in dealing with this issue, in that the training functions of the Local Authority were subject to savings in the same way as other functions. Legal and ICT staff were fully occupied in their day to day roles and could not be released as trainers providing courses on a large scale

9. Fortunately, electronic training materials on data protection compliance have now become available on a Wales wide basis. Officers here have looked at the training material and find that it is suitable for our purposes

and probably an improvement on the paper based training materials used up until now.

10. The training, via the All-Wales Academy, has been rolled out to the HR Division and is shortly to be made available to the Finance & Corporate Services (F&CS) and the Social Services, Health & Housing (SSH&H) Directorates. The system is very user friendly and can be completed in modules which allow staff to train at their own pace and in their own time, stopping and starting as they want, thereby limiting the need for staff to spend large periods of time away from their day jobs. The initial training will cover Handling Information and Information Governance as well as Data Protection matters.

11. The Information Commissioner's Audit also suggested that the Council develop what it termed as "Desk Instructions" for those officers handling Subject Access Requests. These are requests received from individuals requesting the disclosure of personal information held about them. These Desk Instructions were developed some while ago and are reproduced in the appendix to this report.

12. Where unauthorised data releases have occurred it is good practice for the Data Controller to consider self-reporting the releases to the Information Commissioner. The Information Commissioner is now able to fine organisations up to £500,000 for data breaches. In 2015 officers adopted a more formal procedure for the consideration of whether to self-report. Previously the relevant Head of Service made the decision subject to advice from the Head of Legal Services and the Head of Information Technology and Procurement. The procedure which is now adopted is to convene a meeting of the relevant officers and come to a consensus decision based on the relevant criteria. The issues which the Information Commissioner suggests should be considered are the nature and content of the data which has been released, what measures have been put in place subsequently to retrieve and protect the information, and the likely effect on the data subject (ie the person to which the information relates). There has only been one referral to the Information Commissioner in 2015 and this did not give rise to the imposition of a penalty due to the action taken which had been taken to retrieve the data.

13. The Governance Group, which consists of officers from various directorates is considering specifying procedures for mail handling since the reported disclosure.

Financial Impact

14. There is no financial impact on the Authority since the training material was developed on a Wales wide basis.

Equality Impact Assessment

15. This would not be appropriate since this is an information report only.

Workforce Impacts

16. Training for staff on data protection and information handling will be improved.

Legal Impacts

17. The actions taken will secure a greater degree of compliance with the data protection principles.

Risk Management

18. The risk in relation to data protection issues is being dealt with as part of the Councils Risk Management exercise.

Consultation

19. This is not required in this case.

Appendices

20. Appendix 1 - Contains the Data Subject Access Request Desk Instructions

List of Background Papers

21. Information Commissioner Audit.

Officer Contact

David Michael - Head of Legal Services

Tel: 01639 763368 e-mail: d.michael@npt.gov.uk

Stephen John - Head of ICT and Procurement

Tel: 01639 686281 email: s.john@npt.gov.uk

APPENDIX 1
Data Subject Access Request Desk Instructions

DEALING WITH REQUESTS FROM MEMBERS OF THE PUBLIC FOR ACCESS TO THEIR OWN PERSONAL INFORMATION

Introduction

The Data Protection Act 1998 ("the DPA") allows individuals to request a copy of any personal information that is held about them by making what is known as a 'Subject Access Request' (often abbreviated to SARs). Requests for information can also be made on behalf of another person (where the person making the request has legal authority to do so, or where they have the consent of the subject), for example a parent on behalf of their child or a solicitor instructed by their client.

The Council has a legal obligation under the DPA to respond to such requests promptly and in any event, within 40 calendar days of their receipt by the Council. Failure to handle requests correctly may result in complaints being made against us to the Information Commissioner which can lead to enforcement action and even financial penalties being imposed.

Informal Requests

Some requests we receive may be straightforward and can be answered easily. For example, an individual whose identity is obvious to us is asking for a limited and very specific piece of information that they clearly have the right to have. We must therefore adopt a practical approach to requests from individuals. With the person's agreement, requests that take place as part of a normal business can be dealt with informally.

This document sets out the Council's four step process for handling requests for personal information that cannot be dealt with informally. Whilst timescales for completing each step are specified, if it is possible to handle and respond to a request in a shorter time, then we must do so.

Further information in respect to dealing with Subject Access Requests can be found in the Schedule to the Corporate Data Protection Policy which is available on the Authority's Intranet.

STEP 1

The request for information is received

Requests must be received in writing. The request must be date stamped on the day of receipt. The timescale for response begins when the request is received by the Council, not the date it is received by the officer responsible for dealing with it.

Notify the designated Officer and acknowledge request

A designated Officer within each Section of a Directorate should be designated to handle Subject Access Requests relating to that Section. This would normally be an Accountable Manager or other officer of middle management level and they must inform the Directorate's DPA/FOI Co-ordinator immediately when the request is received. A copy should be forwarded by the designated Officer to the Directorate's DPA/FOI Co-ordinator without delay and an acknowledgement letter should be sent to the requester by the Co-ordinator who will log details of the request on the Subject Access Request database maintained by their Directorate.

If a blanket request is received e.g. for "all the information that the Council holds on me" officers should engage with the requester and explain that in order to find the information it would be helpful for the requester to explain which Sections of the Council they have had dealings with. The Council does not retain a central database of all personal information.

Step 1 should be completed within 1–3 working days of receiving the request.

STEP 2

Begin compiling the information

The requested information must be retrieved and compiled as soon as practicably possible by the designated Officer.

Meet with the Head of Service or the Data Protection Officer (Head of Legal Services) or Corporate Solicitor

The designated Officer will discuss the request with the Head of Service if necessary in order to decide which information should be released or if any information should be withheld. The grounds on which access may be refused are referred to in paragraphs 7 and 10 of the Schedule to the Authority's Data Protection Policy which is available on the Authority's Intranet. It might be necessary to involve other officers, for example, the Corporate Solicitor or the Authority's Data Protection Officer (Head of Legal Services) to obtain legal advice on issues arising from the request. However, it is important that any such meeting is arranged swiftly to ensure the final deadline can be met.

Step 2 must be completed within 20 calendar days of receiving the request

STEP 3

Arrange to provide the information

Following the decision as to what information is to be released or withheld, the designated Officer will write to the requester to inform them that the information to which they are entitled to has been retrieved and confirm the method by which the information is to be provided to him/her.

If the requester is agreeable, access may be made available by inspection only, however should the requester require a copy this should be supplied.

In most cases, we will ask the requester to collect the information from a Council office. This is in the interests of security: as it is likely in many cases that the information will contain sensitive personal data that could cause significant distress or even harm if lost or misdirected.

If possible and with their agreement, a meeting can be arranged with the requester to provide an opportunity to explain the information, in order to avoid any misinterpretations, discuss queries etc, relating to the information being disclosed and/or withheld.

Step 3 must be completed within 30 calendar days of receiving the request

STEP 4

Provide the information

Where possible, the information should be collected by the requester or a person acting on their behalf from a Council office or delivered in person by a Council employee, if feasible. Before being provided with the information, the requester or their representative must show proof of identity – the need to do so will have been made clear to them in the letter confirming arrangements for the provision of the information. In compiling information beware of accidentally including personal information about other people.

Information should not be sent via post unless approval is first given by an Accountable Manager and that method of delivery has been specifically requested by the requester. Any information that is posted must be sent via recorded delivery. A written record of delivery must be compiled in respect of any information which is hand delivered (e.g. by whom and when).

As soon as the requested information has been sent or the process for dealing with the request has been completed the designated Officer should inform their Directorate's DPA/FOI Co-ordinator. The Co-Ordinator should be provided with a copy of the response sent to the requester (i.e. the response letter but not any copy documentation including the requested information) and the relevant details will be recorded in the Directorate's Subject Access Request database.

Administrative Practices

Separate files should be set up for each SAR and retained in the Directorate either by the DPA/FOI Co-ordinator or the officer dealing with SARs for the Section. A processing record (see the annex attached) should be compiled and retained by the DPA/FOI Co-ordinator as a basis to provide statistical information.

The file used to process each SAR should be retained for two years. The file should be retained after compliance with the request by the DPA/FOI Co-ordinator.

SARs figures should be notified by the DPA/FOI Co-ordinator to the central contact points in Legal Services every three months Alison Forbes a.forbes@npt.gov.uk Linda White l.white@npt.gov.uk.

The Corporate Solicitor will quality check a sample of SARs and disclosures each year and the Directorate concerned will co-operate with the Corporate Solicitor and allow access to files for that purpose.

Should Officers require legal advice on any aspects of the above guidance they should contact the Authority's Corporate Solicitor by telephone on 01639-763761 or alternatively by email to p.watkins1@npt.gov.uk

ANNEX

Processing Record

Name of Requester:	
Address:	
Email:	
Telephone:	
Nature of Request	
File Reference:	
Date of Request	
Date of Acknowledgment :	
Date of Full Response	
Was all required information provided?	**Yes** ☐ **No** ☐
If no what were the grounds for refusal?	