WEST MIDLANDS FIRE AND RESCUE AUTHORITY

26th NOVEMBER 2012

1. THE DATA PROTECTION ACT 1998

Report of the Clerk to the Authority and Monitoring Officer

RECOMMENDED

That members of the Authority note the contents of the report and the obligations placed on them and the Authority in relation to data protection.

That members of the Authority seek advice from the Director of Human Resources or the Clerk and Monitoring Officer, as appropriate, if they are unsure about any obligations in relation to data protection.

2. PURPOSE OF REPORT

2.1 The purpose of this report is to remind members of the Authority about some of the key requirements of the data protection legislation and guidance. This follows a complaint that was made by an employee to the Information Commissioner's Officer.

3. BACKGROUND

3.1 The Data Protection Act 1998 ("the Act") regulates the holding and processing of personal information that relates to living individuals and which is held on computer or paper. The legislation and numerous associated advice and guidance can seem complex although the important underpinning principles are more straightforward.

3.2 The Act lists the data protection principles in the following terms:

i. Personal data should be processed fairly and lawfully and shall not be processed unless certain conditions are met.
ii. 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.
iii. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are

processed.

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

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

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

vii. 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.

viii. 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.

3.3 Personal data means data which relates to a living individual who can be identified:-

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.4 Sensitive personal data means personal data consisting of information as to:-

a) the racial or ethnic origin of the data subject;
b) his/her political opinions;
c) his/her religious beliefs or other beliefs of a similar nature;
d) whether he/she is a member of a trade union;
e) his/her physical or mental health or condition,
f) his/her sexual life,
g) the commission or alleged commission by him/her of any offence; or
h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

The presumption is that because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

3.5 When a public authority receives a request for information that constitutes personal data about its employees it must decide whether disclosure would breach principle 1 of the Act, ie whether it would be fair and lawful to disclose the information.

Whether the disclosure is fair will depend on a number of factors including:-

- whether it is sensitive personal data;
- the consequences of disclosure;
- the reasonable expectations of the employees; and
- the balance between any legitimate public interest in disclosure and the rights and freedoms of the employees concerned.

If the public authority decides that it would be fair, the disclosure must also satisfy one of the conditions in Schedule 2 of the Act.

In addition, if the information constitutes sensitive personal data, the disclosure must also satisfy one of the conditions in Schedule 3 of the Act.

3.6 Requests for information relating to a public authority's staff can cover a wide range of topics, including the names of staff, organisation charts and internal directories, as well as other data where individual employees can be identified, such as information on salaries and pensions, severance payments and compromise agreements, disciplinary or grievance cases, sickness statistics and training records. Any recorded information held by public authorities that identifies individuals will constitute personal data.

When information relates only to a post, without reference to an identifiable individual who holds that post, it would not constitute personal data. A record that a post with certain responsibilities exists in an authority is not in itself personal data; a record that an individual held a certain post, and therefore had certain responsibilities, is personal data about them.

The job description for a post does not in itself constitute personal data about anyone who may happen to hold that post. However, if the postholder is identifiable from that job description, or from the job description and other available data, for example where the name and job title of the postholder are shown on the authority's website, this is personal data. However, even though a job description may constitute personal data in these circumstances, it is likely that it would be fair to release it in response to a Freedom of Information Act request.

3.7 The elected members of the Authority are likely to have several main roles:-

- they will represent residents of their ward and district;
- they will represent their district authority;
- they will act as a member of the Authority, for example, as a member of a committee;
- they may represent a political party, particularly at election time.

Depending on the role the elected member has at any one time, the Authority may be able to disclose personal information to them. In doing so, it will often be necessary to explicitly restrict the use of any personal information provided for specific purposes.

The Authority can disclose personal information to an elected member if they need to access and use that information to carry out official duties. Elected members are, effectively, in the same position as an employee.

When disclosing personal information to the elected member, the Authority should specify the purposes for which that information may be used or disclosed. This may be done on a case-by-case basis or through developing more general procedures and guidelines.

Where the elected member is able to take a copy of the personal information away from the Authority premises (whether in paper or electronic form), or where they have remote access to the information, the Authority should specify the steps to be taken to keep the information secure. For example, they may lay down rules about how personal information on a laptop or on paper should be stored securely and who can have access to it.

A local authority does not generally have to get the consent of an individual to disclose their personal information to an elected member, as long as:

- the elected member represents the ward in which the individual lives;
- the elected member makes it clear that they are representing the individual for any request for their personal information to the Authority; and
- the information is necessary to respond to the individual's complaint.

Where personal information is particularly sensitive, it may be advisable to get an individual's signed consent. However, there may be circumstances where the individual would reasonably expect their sensitive information to be disclosed to respond to their complaint. In any event when providing personal information to the elected member, the Authority should make clear that it is provided only to help the individual and must not be used for any other purposes. Authorities may wish to do this for each disclosure or more generally by a code of practice for members. It would certainly be good practice to keep a record of any request by elected members for personal information.

Authorities should not normally disclose personal information to elected members for political purposes without the consent of the individuals concerned. There are two exceptions to this:-

- There may be sets of personal information which the Authority is required to make public, for example, lists of some types of licence holder. In this case the Act does not prevent disclosure.
- Personal information may also be disclosed if it is presented in an aggregated form and does not identify any living individuals, for example, Council Tax band information or statistical information. However, there would be a breach of the Act if personal information was released in an apparently anonymised form which could then be linked to the individuals concerned, for example, by comparing property data with the electoral role.

3.8 Data protection law and guidance clearly requires compliance and discipline by both the Authority and elected members. The Information Commissioner's Office website includes detailed

4. EQUALITY IMPACT ASSESSMENT

4.1 An Equality Impact Assessment has not been carried out as this report simply sets out law and guidance in relation to data protection.

5. LEGAL IMPLICATIONS

5.1 The report sets out the main aspects of relevant data protection law and advice. The Act gives the Information Commissioner power to serve a data controller with a monetary penalty notice of up to £500,000 if:

- There has been a serious contravention of any of the data protection principles;
- It was of a kind likely to cause substantial damage or distress; and
- The contravention was deliberate or the data controller knew or ought to have known there was a risk that the contravention would occur and cause damage or distress but failed to take reasonable steps to prevent it. The Information Commissioner's Officer can also conduct audits to establish compliance.

6. FINANCIAL IMPLICATIONS

6.1 There are no financial implications arising directly from this report. Non-compliance with data protection principles could result in the imposition of financial penalties and claims for compensation as well as reputational damage.

N SHARMA
CLERK TO THE AUTHORITY
AND MONITORING OFFICER

Background Papers

www.ico.gov.uk

Data Protection Good Practice Note - Advice to Local Authorities on Disclosing Personal Information to Elected Members

Data Protection Good Practice Note - Advice for the Elected and Prospective Members of Local Authorities.

Requests for Personal Data about Public Authority Employees.
Freedom of Information Act
Environmental Information Regulations