

## **Cabinet – 17 December 2008**

### **Data Protection & Information Security Protocols**

**Portfolio:** Councillor Mohammed Arif, Portfolio Holder for Procurement, Transformation & Performance Management

**Services:** Corporate Performance Management  
Information Communications Technology

**Wards:** All Wards

**Key decision:** No

**Forward plan:** No

#### **1. Summary of report**

- 1.1 The report sets out for Cabinet's consideration two closely related overarching protocols for the council, relating to information security, concerned with all information assets of the council, and data protection, relating to personal data held by the council. These protocols have been developed in the context of an internal review of current practice within the council relating to information security and data protection, to ensure that council policies and procedures in these important areas remain fit for purpose, and so as to address relevant standards, the requirements of the Data Protection Act, and related guidance from the Information Commissioner.

#### **2. Recommendations**

- 2.1 To approve the information security and data protection protocols attached to this report
- 2.2 To note that steps are being taken within the council, and in the community, to ensure awareness and understanding of local arrangements relating to data protection and information security generally, and to ensure compliance with those arrangements.

#### **3. Background information**

- 3.1.1 The council is required to work within the legal framework provided by the Data Protection Act, and the eight data protection principles:
- 3.1.2 Personal data shall be processed fairly, lawfully and, in particular, shall not be processed unless specific conditions are met.

- 3.1.3 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.
- 3.1.4 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- 3.1.5 Personal data shall be accurate and, where necessary, kept up to date.
- 3.1.6 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- 3.1.7 Personal data shall be processed in accordance with the rights of data subjects under the Act.
- 3.1.8 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.
- 3.1.9 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.
- 3.2 Responsibility for data protection matters and for the council's arrangements to ensure compliance with the Data Protection Act transferred from ICT to Corporate Performance Management during 2007/08, and now sit alongside arrangements for Freedom of Information and related matters. Following that transfer, and in the context of the heightened media and public awareness of the importance of systems to ensure that personal information held by public bodies is held, and processed in ways which ensure security and confidentiality, a review of current arrangements has been undertaken, and the opportunity has been taken to revise existing arrangements, in relation to guidance available to residents, clients and service users, and guidance available to council services.
- 3.3 It should be noted that current practices, in place for a number of years, have provided an effective framework and that, as a result, the council has not experienced any significant breaches of data protection legislation. However, in an environment in which data protection and public awareness of personal data has increased, the expectations of government, citizens and those other organisations that work with us, as partners or as contractors, have risen, requiring a more explicit statement of our approach to the legislation, hence the development of the draft data protection protocol attached to this report (**Appendix A**). This protocol is based upon the eight overarching data protection principles, and is set out here for Cabinet's approval.
- 3.4 Likewise, steps have been taken to build upon the existing suite of procedures and processes relating to data protection, set out for staff on the public folder system, to ensure that they meet the needs of all services, and reflect the responsibilities that the council, its services, and individual employees have relating to data protection and the security of personal data that is collected and held by the authority. Greater use is being made of the council's intranet and

steps are in hand to ensure that all staff, at all levels, are aware of the requirements of data protection legislation and their own responsibilities under the Act. Work is also underway to ensure that, in an environment where increasingly the council is working in partnership with others, arrangements for data sharing adhere to the Act and to good practice, in relation to data sharing protocols, where necessary, and in the maintenance of Data Collection (Fair Processing) notices, provided to data subjects when data is collected by the council and its services.

- 3.5 Finally, new internet pages for data protection have been developed to assist residents and other users of our services who may wish to gain access to personal data held by the council about themselves. This supplements existing leaflets, and will be followed up by further public advice and guidance as appropriate.
- 3.6 In addition, it should be noted that the council, corporately and at a service level, holds very significant information assets, personal data and non-personal data, including paper records held in printed documents, notes and files, and other information held electronically, held centrally and on individual PCs. It is important that all information that the council holds is held safely and securely, both to ensure business continuity and to minimise the risk of data loss. In addition to the requirements of data protection legislation, set out above, the protocols set out in this report are informed by the standards ISO/IEC 27002 (based upon ISO/IEC 17799) and ISO/IEC 27001 relating to information security management. The attached information security protocol (**Appendix B**) has been prepared to underpin the council's commitment to effective information security practice across all our services and functions, and in relation to those activities that we undertake jointly with partners.

#### **4. Resource considerations**

##### **4.1 Financial:**

There are no financial implications arising directly from this report.

##### **4.2 Legal:**

Data protection involves the implementation of administrative, technical and physical measures to guard against unauthorised access to personal data. It stems from legislative requirements such as the European Convention for the Protection of Human Rights and Freedoms and has, with the advancement in automated processing of data, been influenced by new legislations such as Directive 1995/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" and the Privacy and Electronic Commerce Directive. It involves the protection of personal data, which covers both facts and opinions about an individual. In the United Kingdom, the influence of these Directives can be seen in the Data Protection Act 1998.

See related comments set out below under Risk.

#### **4.3 Staffing:**

As noted above, responsibility for the council's data protection arrangements rests with Corporate Performance Management, and within that service, arrangements are coordinated by a team of three (2.0 FTE posts) also responsible for Freedom of Information matters including the coordination of requests received.

Data protection and information security are relevant to all members of staff. Specific training and awareness raising will ensure that all staff are aware of their responsibilities in these respects.

### **5. Citizen impact**

5.1 Given the ongoing media focus on data breaches, there is heightened awareness amongst the public with regard to the handling of personal data. Managing personal information effectively should be seen as essential to serving our customers in an acceptable manner. In addition if we ensure data protection compliance is embedded within good information management practices, this will have a range of positive benefits for our customers. These may include:

- Greater confidence in the council and its systems, and less complaints
- Greater visibility of arrangements for subject access requests and their handling
- Reduced risk of an enforcement notice being served on the council due to lack of appropriate processes

### **6. Community safety**

6.1 There are no specific community safety implications arising from this report; however, crime reduction is an area of council activity where council services work in close partnership with other agencies, and where personal data, including sensitive personal information may be held.

### **7. Environmental impact**

7.1 There are no specific community safety implications arising from this report.

### **8. Performance and risk management issues**

#### **8.1 Risk:**

There are three main risk areas:

- *Breach of duty:* The Data Protection Act imposes a duty upon the council to collect, handle (or process) and where appropriate dispose of personal information about citizens, clients and service users, and about our employees, lawfully and correctly, in accordance with the Act. The Act also requires that the council will respond to requests from data subjects for their personal data within 40 calendar days. Without a suitable information management framework and control system in place, there is a risk of a breach of that duty.

- *Corporate governance:* Poor record keeping presents a risk to administrative efficiency and to meeting increasingly complex corporate governance and audit requirements.
- *Digital records:* Although the Act applies to paper based records as well as electronically held information, there is a high level of risk of serious loss of digital (electronic) records if organisational structures do not provide the necessary arrangements for their management and preservation.

While it may be the case that fines for breaches of the Data Protection Act (DPA) and for information security incidents are currently comparatively small, several other things are at risk, including:

- The auditable cost of defending an action for damages
- The auditable cost of defending a criminal prosecution
- The reputation of the organisation
- The risk of not complying with emerging Government requirements on information security, such as eligibility to connect to the new Secure Government Gateway.

## 8.2 Performance management:

Performance should be better managed as a result of the provision of a data protection compliance framework in which to operate in compliance with the legislation. This supports the requirements of providing and maintaining accurate and up to date information; accessed appropriately in a secure fashion. Thus any decisions made on the basis of said information can be attested more fully and any potential damage as a result of a data breach can be minimised.

## 9. Equality implications

- 9.1 There are no particular equality implications arising from this report. Compliance with data protection legislation will help ensure that all citizens and service users, past, present and future, whose personal data is held by the council will have equal access to their own information, should they require it.

## 10. Consultation

- 10.1 All directorates have been consulted as part of these reviews. A range of officers have been interviewed and key documents and procedures from across the council have been assessed. Both data protection and information security are owned by the Information Management Group which contains representation from across the council. This report has already been passed by that group.

The data protection and information security protocols, and this report, have been discussed with trade unions through the Employee Relations Forum.

## Background papers

Article 8 (1) Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol No 11  
 Directive 1995/46/E.C.[1995] O.J. L281/31  
 Directive 2002/58/E.C OJ L 201/37

## Authors

Paul Milmore  
Head of ICT Strategy & Client Services  
☎ 01922 655550  
✉ [milmorep@walsall.gov.uk](mailto:milmorep@walsall.gov.uk)

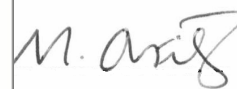
John Pryce-Jones  
Corporate Performance Manager  
(Customer Focus & Intelligence)  
☎ 01922 652077  
✉ [pryce-jonesj@walsall.gov.uk](mailto:pryce-jonesj@walsall.gov.uk)



Tim Johnson  
Executive Director  
December 2008



David Brown  
Executive Director  
December 2008



Councillor Mohammed Arif  
Portfolio holder  
December 2008



**Walsall** Council

**Corporate Data  
Protection Protocol**

# **Walsall Council – Corporate Data Protection Protocol**

## **Overview**

Walsall Council is fully committed to compliance with the Data Protection Act (1998) and recognises the rights and obligations enforced by the act in the processing of personal data within the organisation. This protocol sets out what Walsall Council does to meet the requirements of Data Protection legislation.

## **Introduction**

In order to operate efficiently and effectively, Walsall Council has to collect and use personal information about people with whom it works. These include members of the public, current, past and prospective employees, clients and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

Walsall Council regards the lawful and correct handling of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it provides its services.

## **Scope**

This protocol covers personal data held electronically by Walsall Council on central IT systems and PC's, in addition to data stored in paper files. Personal Data is defined as any information from which a living individual can be identified.

The protocol applies to all council employees, elected members and any other third party who is authorised to process information on behalf of the council.

## **Aim**

The aim of this protocol is to ensure that the council treats personal information lawfully and correctly in accordance with the Data Protection Act 1998 regardless of the format in which it is stored and collected.

## **Owner**

The protocol is owned by the Data Protection Officer



## **Our commitment**

Walsall Council is fully committed to the main principles of the Data Protection Act (1998). When collecting and processing personal data, the following principles will be applied:

**1. Personal data shall be processed fairly, lawfully and, in particular, shall not be processed unless specific conditions are met.**

The council will ensure that the collection and processing of information is not excessive and that it is appropriate to fulfil the operational needs of the organisation or to comply with any legal requirements

**2. 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.**

The council will ensure that when information is collected, on forms or by other methods, specific advice is given as to the purpose(s) of gathering and using the information.

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

The council will ensure the quality and accuracy of any information used, and that any information held is factually relevant to the area of work concerned

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

The council will endeavour to ensure that any personal data is accurate and current and where discrepancies are found, the data will be amended.

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

The council will ensure that any personal information is not held for longer than required and, by applying checks to determine the length of time information is held, make sure that personal data is destroyed in an appropriate manner once the retention period has expired.

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

The council will ensure that an effective process exists to allow data subjects to fully exercise their rights to request to see any of the information held about them within the authority and to ensure that any such request is responded to within the legal time scale of 40 calendar days.

**7. 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.**

The council will ensure that appropriate procedures are in place to safeguard personal information and ensure that access is restricted only to those council officers who require it.

**8. 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.**

Walsall Council will ensure that personal information is not transferred abroad without suitable safeguards.

Walsall Council will also ensure that:

- Our notification entry on the Public Register of Data Controllers is current and up to date. This includes Walsall Metropolitan Borough Council, The Register Office, and The Electoral Register Office of Walsall.
- Any partners or third parties who have access to or share our data follow our policies and procedures and are covered by either a data sharing agreement or outsourcing contract which allows them to lawfully act on our behalf as data processors.
- A dedicated resource is provided to oversee data protection issues across the organisation.
- All council employees (including contractors) involved in the collection and processing of personal data are aware of their legal responsibilities to provide adequate protection of personal information and safeguard against unlawful disclosure.

**Related Legislation and Documentation**

Data Protection Act 1998

Freedom of Information Act 2000

Data Protection Code of Practice (Work in progress)

Corporate Records Management Policy

Corporate Record Retention Schedule



# Walsall Council

Walsall Council's Corporate Management Team and Cabinet intend to develop, implement and comply with the Information Security Protocol set out below. In the interim, until the supporting processes and procedures are developed and communicated, this protocol cannot be fully enforced but the principles and concepts are valid immediately.

## Information Security Protocol

| OBJECTIVE   | OUR COMMITMENT  |
|---|---|
| <p>The objective of information security is to ensure business continuity and minimise damage by preventing and minimising the impact of security incidents.</p>  | <ul style="list-style-type: none"> <li>■ The purpose of the Protocol is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.</li> <li>■ The Corporate Management Team supports the requirements of information security management and has approved this Information Security protocol.</li> <li>■ The organisation is committed to ensure that:</li> </ul>   |
| <p>NOTES</p> <ol style="list-style-type: none"> <li>1. Information includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversation and over the phone.</li> <li>2. The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.</li> <li>3. Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.</li> <li>4. This includes but is not limited to the protection of Intellectual Property Rights, acting in accordance with the Data Protection Act and the recommendations of the Caldicott Committee and</li> </ol> | <ol style="list-style-type: none"> <li>a) Information will be protected against unauthorised access.</li> <li>b) Confidentiality of information will be assured.</li> <li>c) Integrity of information will be maintained.</li> <li>d) Availability of information is ensured as required by the business processes;</li> <li>e) Regulatory and legislative requirements will be met.</li> <li>f) Business continuity plans will be produced, maintained and tested.</li> <li>g) Information security education and training will be available to all staff.</li> <li>h) All breaches of information security, actual or suspected, will be reported and investigated by the Internal Audit Service.</li> </ol> <ul style="list-style-type: none"> <li>■ The implementation of this Protocol is supported by a number of standards including ISO/IEC 27002 (ISO/IEC 17799) and ISO27001:2005. The organisation will comply with the Walsall Council Information Security Protocol together with internally developed policies and procedures which are consistent with ISO/IEC 27002 (ISO/IEC 17799) and ISO27001:2005. These include standards on virus controls and passwords.</li> <li>■ With the exception of information published for public consumption, all users of Walsall information systems must be formally authorised by appointment as a member of staff, or by other process specifically authorised by the Chief Executive. <i>Authorised users</i> will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.</li> <li>■ Business requirements for the availability of information and</li> </ul> |

|   |  |
|---|--|
| <p>preserving Human Rights.</p> <p>5. Business Continuity plans will ensure that information and vital services are available to users whenever they need them.</p> <p>6. Individuals in breach of this Protocol are subject to disciplinary procedures at the instigation of the relevant Director with responsibility for the relevant information system, including referral to the Police where appropriate.</p> <p>7. Responsibility for Data Protection, within the context of the Data Protection Act, is delegated to the DP and FOI Officer.</p> | <p>information systems will be met.</p> <ul style="list-style-type: none"> <li>■ The role and responsibility for managing information security is currently performed by the Head of ICT Strategy and Client Services. The Head of ICT Strategy and Client Services is currently responsible for providing advice and guidance on the implementation of this Protocol.</li> <li>■ All managers are directly responsible for implementing the Protocol within their business areas, and for adherence by their staff.</li> <li>■ It is the responsibility of each employee to adhere to this Protocol – and all relevant supporting policies and procedures.</li> </ul> |
|---|--|

Version 3 00  
Issued December 2008

This Protocol was approved by Cabinet at its meeting on

.....

(This statement will be reviewed at least annually, or as a result of a major change to the organisation.)