INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Data Protection
TO:	Democratic Services Manager	**DATE:**	18 February 2014
C.C.	Chief Executive Deputy Chief Executive (AJ) Head of Finance		

---

1. Introduction

1.1. In accordance with the Audit Plan for 2013/14, an examination of the above subject area has been completed recently and this report is intended to present the findings and conclusions for information and action where appropriate.

1.2. Wherever possible, results obtained have been discussed with the staff involved in the various procedures examined and their views are incorporated, where appropriate, in any recommendations made. My thanks are extended to all concerned for the help and co-operation received during the audit.

2. Scope and Objectives of Audit

2.1. The purpose of the audit examination was to report a level of assurance on the adequacy of the corporate framework in ensuring compliance with the Data Protection Act 1998.

2.2. The examination comprised an evidential risk-based overview of Data Protection governance focusing on the following themes:

- roles and responsibilities
- accuracy of registration
- training
- data collection
- data sharing and disclosure
- subject access
- prevention of unauthorised access
- compliance monitoring

2.3 The examination was conceived as an assignment to be undertaken jointly with the Council's IT audit consultants and used an evaluation model supplied by them (attached as Appendix 1). The scope was mostly confined to the management of Data Protection at corporate level. The findings are based on discussions with Graham Leach, Democratic Services Manager, and examination of relevant documentation and records.

3 Findings

3.1 General Comments

3.1.1 This audit coincided with a planned timetable for a management review of policy and processes relating to Data Protection, Freedom of Information and Environmental Information Regulations. This is scheduled for completion by the end of July 2014.

3.1.2 At the time of the audit, initiatives were already in place to address known issues in areas such as policy updating, awareness management, training and complaints handling.

3.1 Roles and Responsibilities

3.1.1 A three-level hierarchy is in evidence here. The Deputy Chief Executive and Monitoring Officer is designated as the Senior Information Risk Owner for the Council as defined in the information risk management standard ISO 27001. The Democratic Services Manager (also Deputy Monitoring Officer) is designated as corporate Data Protection Officer (DPO).

3.1.2 The DPO role is defined as ensuring that "the position of the Council in relation to personal data is protected". This specifically includes being the central point of control for subject access requests and other requests for disclosure of personal data. Apart from this, the DPO role is defined more as an advisory rather than a corporate leadership one, although in practice this includes recommending Council policy on Data Protection and managing the data controller registration process.

3.1.3 The third level relates are Council staff generally and their responsibilities are coded in a Staff Guidelines document. The document is in printed booklet form only and is not currently published electronically. It is also advised that new starters do not currently receive welcome packs so the Staff Guidelines would not be issued automatically under the standard induction process.

3.1.4 An initiative is known to be in place to implement a software-driven policy awareness solution designed to capture a range of corporate policies. Properly implemented and managed this will be a more effective alternative to welcome packs with features that include enforcing mandatory on-line reading of polices and procedures covered, answering test questions and signing up.

3.1.5 As a practical guide, the Staff Guidelines come across as narrowly focused not recognising that required standards for compliance have become fused with other policies and procedures, including the Information Security and Conduct Policy and subsidiary policies arising from the Government Code of Connection (now Public Sector Network) standards (e.g. Data Handling, Incident Management, Remote Working). Cross-references to these should ideally be incorporated.

3.1.6 Another area that could be usefully covered in the Staff Guidelines a clear statement to pre-empt any confusion with access rights under the Freedom of Information which is sometimes invoked in requests for personal data disclosure.

Risk
Staff may commit personal data breaches due to lack of understanding of their responsibilities and rights of access by other parties.

Recommendations

(1) The Data Protection Staff Guidelines should be reviewed with consideration given to cross-referencing to other relevant policies and legislative/regulatory relationships.

(2) Following review, the Data Protection Staff Guidelines published electronically on the Intranet and incorporated within policies to be released on implementation of the awareness management software solution.

3.2 Accuracy of Registration

3.2.1 Review and renewal of the data controller registration is handled directly by the DPO. The registration details originate from a local authority template of typical purposes and further details added to expand on the relevant activities. These are rarely subject to change – the last significant change was around four years ago when the Council took on on-street car parking enforcement.

3.2.2 A scan of the current registration entry in the Information Commissioner's web site did not raise any queries or indication of omission.

3.3 Training

3.3.1 There is currently no mandatory requirement for staff to undertake training on Data Protection leaving it to the judgement of service managers to establish need. The DPO has traditionally arranged courses with external providers covering Data Protection, Freedom of Information and Environmental Information Regulations.

3.3.2 Training is now being commissioned from Warwickshire County Council Legal Services and will be incorporated in the corporate Learning and Development Programme.

3.3.3 It was also advised that the scope of the corporate induction programme does not include Data Protection or data handling disciplines generally.

3.3.4 An awareness survey undertaken jointly by Internal Audit and Haines Watts had been envisaged as part of the audit, but has been subsequently shelved due to time constraints. It is proposed to pursue this in the 2014/15 audit year targeting those staff who handle personal data on a day-to-day basis.

Risk
Data Protection training is not effectively targeted according to awareness needs

Recommendation
An awareness survey should be commissioned to gauge understanding of Data Protection matters among those staff handling personal data.

3.4 Data Collection

3.4.1 The standard means of complying with the first Data Protection Principle (fair and lawful processing) is the 'privacy notice' provided to the data subject at the point of data collection. Also referred to as 'fair processing notices', these tend in practice to be inserted into advisory clauses and/or declarations in applications forms for services.

3.4.2 This is not an area of compliance that is managed at corporate level and a comprehensive review by Service Area could not be accommodated within this assignment. A brief review of on-line and downloadable forms on the Council's website showed a mixed picture.

3.4.3 In terms of the minimum information that should be imparted (see Appendix 1 Ref. CO4.1), the hackney carriage and resident parking permit application forms came across as fully complying. The Housing Application form, while appearing mostly compliant, fails to make clear that the information supplied may be used to prevent and detect fraud.

3.4.4 The on-line form for reporting an environmental pollution issue comes across as especially weak in this regard.

3.4.5 The above are only examples and to obtain a fuller picture across the board would require a canvass exercise over the Council as a whole.

Risk
The Council may be in breach of fair processing provsions of the Data Protection Act by not giving sufficient details of processing and sharing at the time of personal data collection

Recommendation
A review of personal data collection arrangements should be undertaken across the Council to identify instances where fair processing notices are not provided to proper standard at the point of collection and institute remedial action taken where required.

3.5 Data Sharing and Disclosure

3.5.1 In recognition that systematic data sharing between organisations is widespread, the Information Commissioner has produces a Data Sharing Code of Practice Code that includes checklists for justifying and managing sharing and promotes data sharing agreements as good practice.

3.5.2 Again this is an area not actively managed at corporate level and review by Service Area could not be accommodated within this assignment. It is also noted that the corporate Data Protection Policy makes no provisions on how the Council seeks assurance that organisations with which it systematically shares personal data process the data lawfully and to proper standards.

Risk
Data sharing arrangements may be difficult to justify in case of challenge.

Recommendations

(1) A review of systematic data sharing should be undertaken across the Council to gauge compliance with the Information Commissioner's Code of Practice and recommend formal data sharing agreements where not already applied.

(2) The Data Protection Policy should be updated to reflect systematic data sharing with other organisations and how it is managed.

3.5.3 Requests for disclosure of personal data should normally be routed via the DPO who logs them (the requestors are typically the Police and other local authorities). However, it is not certain to what extent requests are handled directly by the Service Areas without reference to the DPO.

3.5.4 This is seen as bound up with two of the main areas examined – roles/ responsibilities and compliance monitoring. Recommendations made under these areas would be seen as addressing uncertainties about conformance with disclosure request procedures.

3.6 Subject Access

3.6.1 The DPO acts as central point of contact for subject access requests and maintains a spreadsheet log. The DPO also handles responses where the requests are for personal data processed by more than one Service Area.

3.6.2 The volume of incoming subject access requests is not especially high (around 20 over the last twelve months). However, the Council's record in meeting requests within the 40-day statutory timeframe is poor – over the last twelve months the period was exceeded in 85 per cent of cases.

3.6.3 At the time of the audit, a separate investigation was conducted into a particularly extreme case in this regard connected with an unauthorised disclosure that occurred in providing the requested information. It was clear in this case that the critical delays were within the applicable Service Area after the request had been circulated among the managers/team leaders.

3.6.4 This is seen as indicative of a generally low profile for Data Protection among managers when pitted against the service delivery demands, combined with perceived lack of appreciation of the potential consequences of not respecting data subject rights.

3.6.5 What was also noticed in this case, however, is that that almost two week had elapsed after the request date before it had been circulated to the managers/team leaders in the first place. A significant proportion of this time period relates to the forwarding by Democratic Services.

3.6.6 A further observation here is that a tentative request had been received from the same party five weeks before the effective request date but had not been actioned or responded to in the interim. What may be significant is the earlier request invoked the Freedom of Information Act 2000 (FOI) and not the Data Protection Act.

3.6.7 It should be recognised that the average data subject may not understand the distinction between the two and incoming requests should not be assumed to relate to FOI simply because they quote it.

3.6.8 The case also highlighted:

- potential complications where 3rd parties submit requests on behalf of data subjects, especially in circumstances where official complaints are involved;

- possible shortcomings regarding existing redaction methods.

3.6.9 ***Risk***
Continued failure to handle subject access requests in accordance with legislative requirements may lead to reputational damage for the Council and sanctions from the Information Commissioner

Recommendation
The current arrangements for handling subject access requests should be reviewed to determine and implement actions for improving compliance.

3.7 Prevention of Unauthorised Access

3.7.1 The Council's Information Security and Conduct Policy provides the base standards on ensuring that access to personal data is restricted to those persons that can demonstrate a genuine operational need. These are expanded in subsidiary policies relating to specific areas including data handling, e-mail, remote working and removable media.

3.7.2 Access control is evaluated as standard in ongoing audits of all aspects of IT infrastructure, databases, business applications and remote working facilities. A high level of assurance is consistently reported from these audits.

3.7.3 It was advised that the DPO and ICT Services Manager are consulting on a project to implement document marking as a means of improving security arrangements.

3.8 Compliance Monitoring

3.8.1 Absence of effective compliance monitoring is a common area of weakness reported by the Information Commissioner's Office from its reviews of local authorities. It would appear that Warwick District Council is no exception with no tangible framework in place for proactive compliance monitoring.

3.8.2 In the past, the Council instituted network of 'information champions' to help support Data Protection, Freedom of Information and (where applicable) Environmental Information Regulations compliance within the Service Areas. This arrangement effectively lapsed several years ago.

3.8.3 Management should have regard to the need to bring compliance monitoring up to the standard expected by the Information Commissioner's Office and the potential benefits of re-establishing a network of suitably trained Service Area representatives in helping to achieve this.

Risk
Avoidable data breaches may occur through ineffective compliance management over the Council as a whole.

Recommendation
A framework for active monitoring of compliance with Data Protection legislation and good practice should be established with consideration given to reconstituting a network of Service Area representatives.

4 Conclusions

4.1 The overall picture on Data Protection governance shows a mix of strengths, weaknesses and some uncertainties which qualify the level of assurance.

4.2 Taking into account improvement actions in hand, the Council shows itself generally strong in areas such as data controller registration, defining responsibilities, training and access security.

4.3 However, lack of visible corporate leadership on areas such as fair processing and systematic data sharing creates uncertainties that can only be resolved by further review and, in the case of the latter, clearer policies.

4.4 Subject access and compliance monitoring come out as particular areas of weakness.

4.5 In view of the above, the findings only give LIMITED assurance that risks in respect of Data Protection compliance are effectively managed. Further more in-depth review would be a pre-requisite to ascribing a more favourable assurance level.

5 **Management Action**

5.1 The above recommendations are reproduced in the Action Plan (Appendix 2) for management response.

Richard Barr
Audit and Risk Manager