TELFORD & WREKIN COUNCIL

AUDIT COMMITTEE 31 JANUARY 2012

INFORMATION GOVERNANCE UPDATE REPORT TO 1st APRIL to 31st DECEMBER 2011

REPORT OF THE HEAD OF GOVERNANCE

1 PURPOSE

1.1 To present to the Audit Committee an update on the Council's Information Governance activities for the period 1st April – 31st December 2011.

2 RECOMMENDATIONS

2.1 That Members of the Audit Committee note the contents of this update report.

3 SUMMARY

3.1 The Councils Information Governance (IG) function forms part of the responsibilities of Audit & Assurance within the Finance, Audit and Information Governance service delivery unit (see paragraph 4.1.2). IG is a key component of good governance and consists of several aspects:

- Data Protection & Privacy
- Freedom of Information
- Information Security
- Information Sharing & Confidentiality
- Information & Records Management
- Information Quality & Assurance

IG has continued during 2011/12 to support senior managers and service delivery managers with the management of their information governance arrangements.

3.3 This update report follows on from the first annual report presented to the Audit Committee in September and contributes to the Council's assurance framework and good governance.

4 UPDATE INFORMATION

4.1 Background

4.1.1 There are a number of pieces of legislation and good practice standards that govern the IG arrangements of the Council. The work of IG is primarily based on the requirements of the Local Authority Data Handling guidelines, ISO27001 (standard for information security), Data Protection Act 1998, Freedom of Information Act 2000[1] and Environmental Information Regulations 2004.

[1] Full provision of FOI Act 2000 powers were not fully introduced until 1 January 2005

4.1.2 The Local Authority Data Handling Guidelines (stated above) recommend that each local authority should appoint a Senior Information Risk Owner (SIRO). The SIRO should be a representative at senior management level and has responsibility for ensuring that management of information risks are weighed alongside the management of other risks facing the Council such as financial, legal and operational risk. At Telford & Wrekin the nominated SIRO for the period covered by this report was the Head of Governance with the Audit & Assurance Manager designated as the Deputy SIRO. With effect from 4th January 2012 the SIRO responsibility has transferred to Head of Finance (Ken Clarke). Following the consultation on the proposed senior management restructure the SIRO should be confirmed as the Assistant Director – Finance, Audit & Information Governance (Ken Clarke).

4.2 Information Rights

4.2.1 Information rights is a collective name for 3 main pieces of legislation in respect to public sector information, these are:

- **Data Protection Act 1998** – looks at personal information relating to individuals
- **Freedom of Information Act 2000** – encompasses any information held by the Council
- **Environmental Information Regulations 2004** – information with an environmental impact

4.2.2 The IG Team has continued to play a key role in providing assurance that the Council complies with information rights legislation during the period. From April to the end of September IG advised on the application of relevant exemptions in respect to requests received under information rights legislation. From 1st October 2011 it took over responsibility for the administration of all information rights requests on behalf of the Council.

4.2.3 IG also plays a prominent part when the Council receives a subject access request (someone requesting their personal information) or a request to access social care records, e.g. a parent asking to view the contents of their child's records. The Councils Data Protection Officer (part of IG Team) gives guidance on what records should or should not be released under the Data Protection Act 1998.

4.2.4 The ICO has set a benchmark of 80% for responding to FOI requests within the 20 day statutory deadline for responding to requests.

4.2.5 For the period April – end of September 2011 450 FOI requests were received, an average of 75 requests per month. 86% of these requests were answered within the 20 working day statutory deadline with the average time to respond to each request being 12 days.

4.2.6 For the period October – end of December 2011 198 FOI requests had been received, an average of 66 requests per month. 83% of these requests were answered within 20 days with the average time to respond to each request being 10 days.

4.3 Data Security Incidents

4.3.1 IG investigates all instances of alleged data breaches that are identified and referred to them. A data breach can cover a number of different incidents from a member/employee

reporting a lost Blackberry to confidential/sensitive information being communicated to an unauthorised and/or incorrect recipient.

4.3.2 Between 1 April and 31 December 2011 there were 46 reported instances of possible data breaches. IG investigated all of these and has as at 6th January 2012 confirmed that 20 data breaches had occurred. These are shown below categorised by type of breach.

	Number of cases	Number of Data Subjects
Information accidentally sent to the incorrect recipient	15	17
Accidental release of personal information verbally	3	3
Documents containing sensitive information left in an insecure location	1	15
Documents containing sensitive information disposed of inappropriately	1	115
Total	20	

4.3.3 For each of these breaches IG agreed actions with the relevant management team to minimise the impact of the breach on the customer. The Council has also changed procedures and provided training to reduce the possibility of similar data breaches occurring in the future. Disciplinary action has been taken in three cases and 2 members of staff have resigned during these processes.

4.3.4 The circumstances for two of the confirmed data breaches met the ICO's notification rationale and were referred to the Information Commissioners Office (ICO). We are still waiting for the ICO's final response to these including any action he requires the Council to take. The Council also informed the ICO of another case due to the extensive local press coverage it received.

4.3.5 In November 2011 Big Brother Watch issued a report compiled from responses to an FOI request – Local Authority Data Losses July 2008 – July 2011. They received a response rate of 91% to the request (395 authorities) and one third reported data losses (132) with two thirds reporting no data losses (263). T&W reported 30 data losses[2] during this period which resulted in us being 9th out of the 132 authorities who reported data losses. Although in comparison with other authorities this may appear high, there are positives to be taken in that the Council has demonstrated an open culture where staff feel comfortable in reporting information security incidents. Also given the recent changes in organisational structure and level of staffing the risks around information security have increased. To help to address this during 2010/11 and continuing into 2011/12 the Council has restructured and expanded the Information Governance function and is continuing the implementation of improved processes, training and awareness across the Council.

4.3.6 Any lessons that should be learnt from data security incidents are shared locally with appropriate employees and across the Council where these lessons apply to all services.

[2] Further analysis of some of the cases submitted found that they had not eventually been confirmed as data breaches. There were 20 confirmed data breaches

4.4 Audit of Information Governance (IG)

4.4.1 An internal audit of the Councils arrangements for IG was completed in March 2011. The report gave the following opinion of the IG arrangements at that time:

*'On the basis of the work carried out it is our opinion that the level of assurance provided by controls for this audit area is Reasonable; t**here is a sound system of control but there is evidence of non compliance with some of the controls. There are Policy/Procedure recommendations and many best practice recommendations that Audit Services are confident that management will implement.**'*

An action plan has been agreed as a result of this audit report. IG has, or is in the process of, implementing actions agreed within the timescales set.

4.5 Information Governance Work Programme

4.5.1 The IG team in addition to the administration of information rights legislation, the investigation of data security breaches set down a work programme to further improve the information governance framework of the Council. Progress to date is shown below:

Action	Progress
Production of a fit for purpose publication scheme	Scheme due for full implementation in January 2012.
Development of a FOI disclosure log	Disclosure log now posted on Councils website and updated monthly
Review of Corporate Information Security Policy (CISP)	The policy has been reviewed and a current pilot taking place re: the online acceptance of this policy.
Follow up of the implementation of the actions from the 2010/11 Safeguarding review	During 2010/11 a review was undertaken in respect to the file/record management arrangements implemented by Safeguarding at The Mount. Actions were agreed with management some of which were implemented by 31st March 2011. A review of the progress to implement the outstanding actions was undertaken during September-October 2011. Implementation is progressing according to agreed timetables with only long term actions still to be implemented.
Developing training and awareness	A number of actions have taken place on this including: Attended SMT to launch awareness programme September 2011 The IG & Risk Team Leader attending a number of Heads of Service management meetings to raise awareness. Current pilot of e learning package intended for full roll out and completion by all council officers

	Targeted training undertaken in higher risk areas such as Safeguarding. New posters currently being developed and due for distribution by the end of January 2012. Members sessions in November 2011 Presentation to all Finance officers in December 2011.
Online agreement to abide by requirements of the CISP	See above.
Guidance on undertaking Privacy Impact Assessments	Guidance now complete and communicated to Project Officers in ICT.

4.5.2 The next update to the Audit Committee on Information Governance will be the 2011/12 Annual report, incorporating activity during January – March 2012 which will be presented to the June Audit Committee.

5 OTHER CONSIDERATIONS

AREA	COMMENTS
Equal Opportunities	All members of the IG Team have attended equal opportunities/diversity training. If any such issues were highlighted as part of IG work they would be notified to the appropriate manager.
Environmental Impact	All members of the IG Team are environmentally aware and if any issues were highlighted as part of IG work they would be notified to the appropriate manager.
Legal Implications	Compliance with the legislation mentioned in this report is mandatory. When assessing compliance, the ICO will consider approved policies and procedures of the authority.
Links with Corporate Priorities	IG is a key component of good governance and links to all corporate priorities.
Risks and Opportunities	The role of IG includes reviewing information security arrangements in place to manage IG risks within service areas. IG reports produced assist the Council in improving systems and controls (reducing IG risks) and therefore the delivery of services and achievement of objectives. If the Council does not comply with the information rights legal requirements there is the risk of the Council being issued with a fine by the ICO of up to £500,000. Service areas supported by the IG Team have and are continuing to implement mitigation to avoid this but there is still risk associated with this.
Financial Implications	IG operated within the Audit & Assurance budget for 2010/11 and is on target to do the same for 2011/12. However if the ICO found that the Council was not complying with the information rights legal requirements and a fine was imposed there is no budget allocation identified to meet this.
Ward Implications	IG is responsible for the IG arrangements all the Council's activities and at all Council locations. They therefore operate within all Council Wards.

Report by Jenny Marriott, Audit & Assurance Manager 383101