

## **TELFORD & WREKIN COUNCIL**

**AUDIT COMMITTEE 25<sup>th</sup> JUNE 2013**

**2012/13 INTERNAL AUDIT AND INFORMATION GOVERNANCE ANNUAL REPORT**

**REPORT OF THE AUDIT & INFORMATION GOVERNANCE MANAGER**

### **1 PURPOSE**

- 1.1 To present the 2012/13 Internal Audit and Information Governance Annual Report to the members of the Audit Committee.

### **2 RECOMMENDATIONS**

- 2.1 That members of the Audit Committee note the 2012/13 Internal Audit and Information Governance Annual Report.

### **3 SUMMARY**

- 3.1 To continue to demonstrate good governance and support the Annual Governance Statement (AGS) the Council produces an Annual Report on the Internal Audit and Information Governance activities of the Council.
- 3.2 The CIPFA Code of Practice for Internal Audit in Local Government in the UK 2006 (the Code)<sup>1</sup>, which has been deemed as proper internal control practice under the Accounts and Audit (England) Regulations 2011, states under Standard 10 – Reporting, that “the Head of Internal Audit must provide a written report to those charged with governance timed to support the Statement on Internal Control”. This report meets this requirement.
- 3.3 The Councils Information Governance (IG) function forms part of the responsibilities of Audit & Information Governance within the Finance, Audit and Information Governance service delivery unit. 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

During 2012/13 IG has continued to support senior managers and service delivery managers with the management of their information governance arrangements.

### **4 PREVIOUS MINUTES**

- 4.1 Audit Committee 16<sup>th</sup> June 2009 – Annual report 2008/09  
Audit Committee 28<sup>th</sup> June 2010 – Annual report 2009/10

---

<sup>1</sup> The Code was superseded on 1<sup>st</sup> April 2013 with the Public Sector Internal Audit Standards which apply from that date.

## 5 2012/13 INTERNAL AUDIT ANNUAL REPORT

### 5.1 Assurance and Opinion on the Systems of Internal Control

- 5.1.1 The Council's section 151 officer's statutory obligation under the Accounts and Audit (England) Regulations 2011 to provide assurance on the systems of internal control is provided by the work of internal audit. This assurance forms part of the Council's assurance framework.
- 5.1.2 The system of internal control helps the Council to manage and control the risks which could affect the achievement of its priorities and objectives rather than eliminate them completely. Internal Audit and the other assurance processes therefore provide reasonable and not absolute assurance of the adequacy and effectiveness of the systems of internal control within the Annual Governance Statement.
- 5.1.3 The planned Internal Audit resources for 2012/13 were 1032 days plus 58 days specialist ICT audit provided under contract (from an external provider). These resources were just over 8% less than for 2011/12 (1193 compared to 1090) due to the full implementation of the Audit & IG team restructure. These revised resources and the plan were agreed by the Audit Committee in March 2012. The actual resources available were similar to those planned (minor reduction due to gap between Auditor leaving and new one starting) but some resources were diverted from Internal Audit work due to work on Ombudsman complaints (13), Public health transfer (27), recruitment – Auditor (5), accommodation move (9) and assistance to Family & Cohesion services (6).
- 5.1.4 Based on the work undertaken during the year (main areas attached as **Appendix A**) and the implementation by management of the agreed recommendations Internal Audit can provide reasonable assurance that the systems of internal control within these areas of the Council were operating adequately and effectively when reviewed during the year. Where necessary the Audit Committee invited Senior Management to explain why progress on the implementation of recommendations were not as agreed and appropriate assurance was provided (or further information is to be provided to the Audit Committee).
- 5.1.5 The previous Internal Audit Annual Report included information in respect to the type and number of recommendations made during the year (as requested by the Committee). This information has continued to be collected for 2012/13 and is shown below with comparisons to 2011/12 shown in brackets.

#### Number of Recommendations made by Type 2012/13 (2011/12)

No. of Audit Reports & Grading	Total number of recommendations	Financial Regulation or DCSF Requirement (schools only)	Legal	Policy and/or Procedure	Best Practice
<b>60 (44)</b>	<b>693 (416)</b>				
<b>9 (11) Green</b>		<b>157</b>	<b>41</b>	<b>416</b>	<b>79</b>
<b>32 (30) Yellow</b>		<b>(63)</b>	<b>(29)</b>	<b>(288)</b>	<b>(36)</b>
<b>14 (3) Amber</b>					
<b>2 (0) Red</b>					
<b>3 various* gradings</b>					

Gradings - Green = good; Yellow = reasonable; Amber = limited; Red = poor

\*3 reports with various levels of assurance (details below)

**Network Infrastructure Report** - Network Infrastructure - Amber, Virus protection - Yellow, Data Centre - Yellow, Wireless Network - Green

**IT Service Design** - Strategy - Yellow, Service Delivery - Yellow, Capacity - Amber

**Cash Collection** - Cash Management - Yellow, Darby house Reception - Yellow, Wellington First Point (Library) - Amber, Legal Services Search Fees - Yellow, Youth & Cohesion (Stafford Park) – Amber

5.1.6 60 reports were issued during 2012/13, 16 more than in 11/12. This is probably due to the scope and complexity of the audits, less unplanned/irregularity type work (53 days in 11/12) and improved processes/efficiency within the team.

5.1.7 Out of the 57 reports (excluding the various grading reports) 16% were green (good), 56% were yellow (reasonable), 25% were amber (limited) and 3% were red (poor). Summary amber and red reports and explanations have been reported to the Committee with detailed reports being circulated to members of the Committee prior to the meeting.

5.1.8 29% of the 12/13 recommendations were legal/financial regulation compared to 22% in 11/12. 60% of the 12/13 recommendations were policy and procedure compared to 69% in 11/12. This again outlines the impacts of organisational change, restructures and the reduced familiarity of staff in new roles.

## 5.2 Performance against External Review

5.2.1 KPMG has been the Council's External Auditors since 1st April 2007. There is continuous liaison between Internal and External Audit to ensure that Internal Audit is undertaking appropriate work upon which the External Auditor can rely and reduce the external audit fee. Internal Audit has delivered all the work for 2012/13 by the end of March 2013 upon which External Audit places reliance to a good standard.

5.2.2 In order to place reliance on the work of Internal Audit the External Auditor assesses the performance of Internal Audit each year against the CIPFA Code (see 3.2). KPMG have undertaken the 2012/13 review and a summary of the findings will be presented to the Committee as part of their interim review feedback. There has been no indication from KPMG of any adverse findings but any actions required will be incorporated into the Internal Audit 13/14 key tasks list. This external review has also been used to meet the requirement of the Accounts and Audit (England) Regulations 2011 for an annual review of internal audit.

## 5.3 Local Performance

5.3.1 Internal Audit has retained 2 local performance indicators. The results with explanations are shown below.

PI Ref	Definition	Outturn 09/10	Outturn 10/11	Outturn 11/12	Target 12/13	Outturn 12/13	Comments/Explanation
LAUD1	% of completed work for the external auditor	100.00	100.00	100.00	100.00	100.00	Achieved

LAUD2	% Planned work completed	90.00	92.00	90.00	92.00	91.70	Slight under achievement due to reasons in para.5.1.3
-------	--------------------------	-------	-------	-------	-------	-------	---

5.3.2 During the year to improve the team's efficiency, effectiveness and productivity we have held team meetings and development sessions. At these sessions and continually during the year we investigate and implement new/alternative ways of service delivery (practices, use of technology, procedures and standard documentation) based on our analysis, customer feedback (see 5.4), sharing best practice with other local authorities and service providers.

5.3.3 The team has also achieved the staff and non-staff savings put forward in addition to the previous savings made (23.3% staff savings (target 20%) and 20% non-staff savings).

5.3.4 Internal Audit is a member of the CIPFA benchmarking club (membership of 147 local authorities). A report was presented to the Audit Committee in January 2013 providing the results which showed that Internal Audit compares positively against other unitary authorities.

5.3.5 The Audit & Information Governance Manager is the Unitary and District representative on the CIPFA Audit Panel. This helps the team to continue to develop and have early awareness of developments in public sector Internal Audit and Governance enabling them to contribute to and influence relevant guidance.

## 5.4 Customer Feedback

5.4.1 Internal Audit receives customer feedback in several ways:-

- a) Informal feedback from auditees during the audit
- b) Seeking feedback from auditees at draft report discussion meetings
- c) Completion of a post audit questionnaire

5.4.2 The analysis of post audit questionnaire feedback is shown in the table below compared to the last 3 years.

### POST AUDIT QUESTIONNAIRE FEEDBACK 2012/13 compared to last 3 years

Question	2009/10 from top score 5	2010/11 from top score 5	2011/12 from top score 5	2012/13 From top score 5	Difference 11/12 to 12/13
Pre- Audit Arrangements	4.6	4.8	4.8	4.6	-0.2
Audit Visit	4.8	4.8	4.6	4.7	+0.1
Communication	4.3	4.5	4.8	4.5	-0.3
Report	4.7	4.7	4.7	4.5	-0.2
Is audit a positive support – Yes	100%	100%	100%	100%	No change

5.4.3 The team continues to perform well with all average scores of 4.5 or more out of 5. However although the audit visit score has increased slightly the other areas have

reduced by between 4 and 6%. The team has reviewed these scores and where additional information has been provided in the feedback changes have been made, where appropriate.

## 6. 2012/13 INFORMATION GOVERNANCE ANNUAL REPORT

### 6.1 Background

6.1.1 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<sup>2</sup> and Environmental Information Regulations 2004.

6.1.2 The Local Authority Data Handling Guidelines 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 is the Assistant Director: Finance, Audit & Information Governance with the Audit & Information Governance Service Delivery Manager designated as the Deputy SIRO.

### 6.2 Information Rights

6.2.1 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

6.2.2 The IG Team has continued to play a key role in providing assurance that the Council complies with information rights legislation during the year. The IG Team has responsibility for the administration of all information rights requests on behalf of the Council including the application of relevant exemptions in respect to requests received.

6.2.3 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 Council's Data Protection Officer (part of IG Team) gives guidance on what records should or should not be released under the Data Protection Act 1998.

6.2.4 The ICO has set a benchmark of 80% for responding to FOI requests within the 20 working day statutory deadline for responding to requests. The table below sets out the figures relating to FOI performance for the year 1 April 2012 to end of March 2013 compared with the same period for the previous year:

---

<sup>2</sup> Full provision of FOI Act 2000 powers were not fully introduced until 1 January 2005

	12/13	11/12	% Increase / Decrease
Number of FOI requests received	862	898	-4%
Average number of FOI requests received per month	72	75	-4%
% of FOI requests responded to within statutory deadline	90	86	+4%
Average time taken (days) to respond to each request	10	12	-20%

As can be seen from the figures in the table above, IG performance in responding to FOI requests has improved and compares favourably with the ICO benchmark of responding to 80% of FOI requests received with 20 working days.

6.2.5 In this period we have received and responded to 11 appeals from requestors who were not satisfied with the response they received to their FOI request. This is a reduction of a total of 9 appeals (45%) from the previous year. This demonstrates a general improvement in the quality of responses to FOI requests sent by the IG team.

6.2.6 Also in this period we received 1 referral from the Information Commissioner (ICO) in respect to a complaint made to them by an FOI requestor. The requestor was not satisfied that the IG team had withheld elements of the information they had requested by applying the appropriate exemptions as detailed in the FOI Act 2000. The ICO initially upheld the requestor's complaint but the Council appealed the ICO's decision. The Council's appeal was upheld with the tribunal stating that we had correctly applied the relevant FOI exemptions.

6.2.7 Between 1 April 2012 and 31 March 2013 we received 65 Subject Access Requests<sup>3</sup> (SAR's) compared to 95 requests for the same period in the previous year. 82% of SAR's received have been processed within the 40 calendar day deadline (71% of SAR's processed within deadline for 2011/12). This is a positive improvement in performance and now compares favourably with the Information Commissioner's benchmark of responding to 80% of SAR's within 40 calendar days.

### 6.3 Data Security Incidents

6.3.1 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.

6.3.2 Between the 1 April 2012 and 31 March 2013 there were 97 reported instances of possible data breaches (77 reported instances in 2011/12). IG investigated all of these and has confirmed that 51 data breaches had occurred (40 data breaches were identified in 2011/12). These are shown below categorised by type of breach:

	Number of Cases	Number of Complaints/Referrals from Data Subjects
Information accidentally sent/made available to the incorrect recipient	<b>44</b> (31 in 11/12)	<b>25</b>
Accidental release of personal information verbally	<b>3</b> (3 in 11/12)	<b>2</b>

<sup>3</sup> A request by an individual for personal information that relates to them or their children

Documents containing sensitive information left in an insecure location	<b>1</b> (1 in 11/12)	<b>1</b>
Documents/information containing sensitive information disposed of inappropriately	<b>0</b> (2 in 11/12)	<b>0</b>
Information lost or stolen	<b>3</b> (3 in 11/12)	<b>0</b>
<b>TOTAL</b>	<b>51</b> (40 in 11/12)	

6.3.3 None of the data breaches detailed above met the Information Commissioner's rationale for reporting serious breaches to them.

6.3.4 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 3 cases:

- 2 officers have received warning letters
- 1 officer resigned during the disciplinary process

In addition to this 1 further officer is currently being investigated under the Council's disciplinary rules. The outcome of this investigation is yet to be determined.

6.3.5 Any lessons learnt from data security incidents are shared locally with appropriate employees. In addition to this the IG Team communicates half yearly lessons learnt highlighted by data breach investigations to all services across the Council – the lessons learnt from October 2012 – March 2013 are attached as Appendix B for information.

6.3.6 The IG Team has received one referral from the Information Commissioner in respect to a complaint made to them by a member of the public affected by one of the data breaches detailed in 6.3.2. This related to a Sales Ledger invoice being sent to an incorrect address. After receiving requested information from the Council in respect to this breach the Information Commissioner was satisfied with our response and the changes made and further plans in place for improvements for processing personal information in this area and no further action was required.

6.3.7 The IG Team also received correspondence in 2012/13 from the Information Commissioners Office (ICO) in respect to 2 data breaches, see details below.

**Breach 1** – Wrekin Housing Trust (WHT) Officer left social care information (including police information) at an individual's home in error.

This incident occurred in 2011/12 and was notified to the ICO by WHT. The ICO contacted the Council in 2012/13 querying why we had not notified them of this incident. The Council provided a response which satisfied the ICO's query and no further action was required.

**Breach 2** – An employee of a care company that the Council contract with had their car stolen. Personal information relating to care clients had been left in the car (information for T&W related to the names of 14 clients). The care company had notified the ICO of this incident.

The ICO contacted the Council and requested additional information in respect to the relationship the Council had with the care company. The ICO were satisfied with the response provided by the Council and no further action was required.

6.3.8 As reported to the Audit Committee on 25/9/12 the ICO fined the Council £90,000<sup>4</sup> in June 2012 for two data breaches notified to the ICO by the Council in May 2011.

#### **6.4 Information Governance Work Programme**

6.4.1 The IG Team, in addition to the administration of information rights legislation and the investigation of data security breaches, set down a work programme to further improve the information governance framework of the Council. The 2012/13 IG work programme was agreed at the March 2012 Audit Committee. Detailed progress to date in respect to this programme is shown in Appendix C.

6.4.2 The next update to the Audit Committee on Information Governance will be the 2013/14 update report, incorporating activity during April – end of August 2013 which will be presented to the September Audit Committee.

### **7 CONCLUSIONS FOR 2012/13**

7.1 Despite limited resources the Internal Audit & IG Team has achieved good results and contributed to the governance arrangements within the Council.

7.2 The statutory responsibilities of the Council's Chief Financial Officer (section 151 officer) to provide an adequate internal audit service have been met and Internal Audit has provided reasonable assurance to the Council on the internal control systems for the areas reviewed in 2012/13.

7.3 Internal Audit and Information Governance Team has also continued to provide advice and guidance on procedures, controls, information security and risk management.

7.4 However, there are numerous major changes occurring both within and outside the Council during 2013/14 which could affect the team's activities, for example :-

- a) The Public Sector Internal Audit Standards became operative from 1<sup>st</sup> April 2013. We have commenced the process to review our practices and reporting requirements against them and will update/introduce new procedures where appropriate including improved quality review (internal and external).
- b) The pressure on the Council's budget strategy for 13/14 has resulted in further savings being put forward including a voluntary reduction in the Service Delivery Manager's resources. It is anticipated that the effect of this on Internal Audit work will be limited as the reduction is being realised by a reduction in corporate work;
- c) Further service restructures and re-engineering, revised governance arrangements and reduced supervisory levels;
- d) The continued development of relationships with revised service delivery areas to ensure the team continues to support the authority in achieving its objectives.
- e) Changes to legislation and the Government's expectations of local government and its policies;
- f) Consideration of the future changes to the external audit and inspection regime;
- g) The Council's key projects including Building Schools for the Future, Waste, Commercial Projects (including the Housing Investment programme) and Single Status.

---

<sup>4</sup> Reduced to £72,000 for prompt payment

## 8 OTHER CONSIDERATIONS

AREA	COMMENTS
Equal Opportunities	All members of the Audit & IG Team have attended equal opportunities/ diversity training. If any such issues arose during any work the appropriate manager would be notified.
Environmental Impact	All members of the Audit & IG Team are environmentally aware and if any issues were identified they would be notified to the appropriate manager.
Legal Implications	<p>The Accounts and Audit (England) Regulations 2011 state that the Council must undertake an adequate and effective internal audit of its accounting records and of its system of internal control in accordance with the proper practices in relation to internal control. There is also a requirement to comply with CIPFA's Code of Practice for Internal Audit in Local Government. Undertaking the audits as set out in the report and providing updates and an Annual Report to this Committee contributes towards meeting these requirements.</p> <p>Further reference to legal requirements and the implementation of those legal requirements in accordance with CIPFA guidance are contained within the main body of the report at paragraphs 3.2, 5.1.1 and 5.2.2 respectively.</p> <p>In the event that an audit reveals an issue which requires a recommendation concerning a legal matter this can also be referred to the Council's Legal Services Team for further advice and assistance.</p> <p>Compliance with the Information Rights legislation mentioned in this report is mandatory. When assessing compliance, the ICO will consider approved policies and procedures of the authority.</p>
Links with Corporate Priorities	All aspects of the Audit & IG teams work support good governance which underpins the achievement of the Council's objectives and quality service delivery.
Risks and Opportunities	<p>All aspects of the Audit &amp; IG teams work supports managers and the Council to identify and manage their risks and opportunities.</p> <p>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.</p> <p>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.</p>
Financial Implications	<p>Audit &amp; IG operated within budget for 2012/13 with an under spend at the end of the year. Where recommendations are made by team members following reviews, if possible, cost implications are identified.</p> <p>The budget for external audit was also under spent for 2012/13 by £90k due to a reduction in the main audit fee.</p> <p>It should be noted that 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.</p>
Ward Implications	The work of the Audit & IG team encompasses all the Council's activities across the Borough and therefore it operates within all Council Wards.

**9     BACKGROUND PAPERS**

Annual Audit Plan 2012/13 and strategy

Internal Audit Action Plan 2012/13

CIPFA Benchmarking Information 2012

Corporate Information Security Policy

Corporate Information Security Breach Procedure

Report by Jenny Marriott, Audit & Information Governance Manager. Telephone: 383101

## MAIN AREAS OF INTERNAL AUDIT WORK UNDERTAKEN 2012/13

Areas	Days
16+ Commissioning	11
Abacus system review	12
Abraham Darby Leisure Centre	13
Accommodation project	1
Advice and Guidance	62
Annual Governance Statement assurance and certification	11
Apley Wood Primary	6
Aqueduct School	6
Arthog	17
Bank contract review	5
Benefits - Workbook sample test	5
Building Schools for the Future	3
Building control fees	2
Car Parking Enforcement	6
Care first application review	4
Cash Collection - general	16
Catering	15
Children's Commissioning	8
Children's Placements	17
Church Aston School	5
Continuing Healthcare	5
Contract changes & waivers of SOs	11
Corporate Parenting expenditure check	4
Council Tax / NNDR	34
Carbon Reduction Commitment review	6
Customer Relationship Management system	3
Dept of Transport grant review	1
Donnington Wood Infants School	5
Early Intervention imprest check	4
Electronic Client Records	4
External IT Audit Contract Management & Procurement	7
Follow ups (including ICT)	19
Foster Carers Form F review	6
Foster carers recruitment campaign	1
Fraud & Compliance Checks	10
Graphical Information Systems review	4
Homelessness Thresholds	6
HR Allowances	9
HR/Payroll	31
ICT Equipment	1
ICT Governance of projects	2
ICT Procurement	2
Infrastructure Project review	1
Insurance	7
Integrated Benefits System	20

John Fletcher of Madeley Primary School	5
Licensing	5
Lightmoor /reflexions overpayment	3
Lilleshall Primary School	8
Main Accounting system	26
Markets & Cash collection	1
Mileage/overtime checks	5
Newdale Nursery and First Steps system	7
Newport Infants School	8
Oakengates Tennis Centre contract	11
P2P and Purchase Ledger	30
PFI facilities management contract review	3
Performance Indicator Verification	3
Planning Applications	2
Procurement	7
Property & Design Helpdesk	12
Pupil Tracking	3
Replacement Jacobs/consultancy	2
Revised School Audit programme	5
Risk management	1
Safe checks	2
Sales Ledger	47
School Funds	1
Self Directed support	2
Service User Journey	4
Shortwood School	5
St Lawrence Primary School	4
St Peters & Pauls School	3
St Peters Edmond School	8
Stage 1 Complaints Correspondence Checks	2
Supportive Lodgings	3
Teagues Bridge School	7
Teenage pregnancy Governance	4
Term Contract / Service Contracts	5
The Bridge Special school	7
Tibberton School	6
Town Park Visitors Centre	6
Trading standards	2
Transparency Agenda	2
Treasury Management	10
Uniform system	5
Voluntary Sector Agreements	1
Wellington Office & Leisure centre accommodation	6
Wrekin View Primary School	8

## Information Security Incidents: Lessons Learnt – 2012/13

### Information Governance (IG) 2<sup>nd</sup> Half Yearly Update – 1 October to 31 March 2013

Information on lessons learnt in respect to data breaches investigated for the first half of 2012/13 were included in the weekly Briefing Note for Managers dated 11/10/12 and Staff News on 19/10/12.

Despite further training/publicity the Council has continued to experience data breaches. These breaches have been investigated by the IG team/service areas and changes to processes have been agreed. However there are lessons to be learnt by us all from these breaches and this note aims to share them with you.



### Top 5 reasons for data breaches at Telford & Wrekin

1

Emails sent to incorrect recipients

2

Officers not completely following agreed processes/procedure

3

Officers basing decision on assumptions rather than fact

4

Use of paperclips to accidentally clip together unrelated information

5

Human error – typing errors, lack of checking contact details, etc.

### What is the impact of these data breaches?

- **Fact:** We have given out someone's bank details to another individual in error – **possible impact: identity theft, financial fraud, etc.**
- **Fact:** We have given out the contact details for a victim of domestic abuse in error – **possible impact: the alleged abuser nearly received these details which could have put the victim in significant danger.**
- **Fact:** One individual affected by a data breach complained to the Information Commissioner – **possible impact: Council could have been fined £500,000, further internal investigation and disciplinary action against employee.**



### Lessons learnt from data breaches



Always check you are emailing who you think you are emailing particularly when the email address auto-populates in Outlook

- ✓ If you are sending an email to a group email address check all the officers in that group are authorised to receive it
- ✓ Ensure you are fully aware of, and abide by, your local procedures and applicable corporate policies such as the Corporate Information Security Policy (CISP)
- ✓ When dealing with personal information NEVER assume. Think what the impact could be of your assumption. All your decisions need to be based on fact.
- ✓ Be careful when sorting personal information for different individuals at the same time. Never use paperclips to separate documents, always consider using plastic wallets
- ✓ When sending correspondence to individuals always double check the address stated on your letter with the source address on your records. Remember house number 82 can easily be quoted as 28 by mistake. But this mistake can be picked up by checking

### £££'s - Top 3 latest fines for local authorities nationally

<p><b>Lewisham - £70,000</b> <i>December 2012</i></p> <p>A social worker left sensitive documents in a plastic shopping bag on a train, after taking them home to work on. The files, which were later, recovered from the rail company's lost property office, included GP and police reports and allegations of sexual abuse and neglect.</p>	<p><b>Plymouth - £60,000</b> <i>November 2012</i></p> <p>An employee at Plymouth Council collected three pages of sensitive information from a printer alongside another document by accident. These documents were then sent out at the same time to one family who received details about a family that wasn't related to them.</p>	<p><b>Devon - £90,000</b> <i>October 2012</i></p> <p>An employee used a previous case as a template for an adoption panel report they were writing up, but sent out a copy of the old report instead of the new one, leaking data on 22 people. That data breach saw details of mental and physical health exposed.</p>
---	---	---

**Remember: Protecting personal information is everybody's responsibility**

**INFORMATION GOVERNANCE WORK PROGRAMME  
PROGRESS AND PROGRAMMED WORK**

<b>No</b>	<b>Task</b>	<b>Completion Date &amp; Comments</b>
1	Administer FOI/EIR/DPA requests, appeals, complaints and associated correspondence from the ICO	Ongoing
2	<p>Deliver IG training and awareness programme and ensure the content of the induction programme is appropriate.</p> <p>Annual refresher training</p>	<p>Ongoing</p> <p>Draft IG module designed for Learning Pool – looking to implement by end of May 2013.</p>
3	<p>Keep the IG and security framework up to date including the Corporate Information Security Policy and associated procedures.</p> <p>Disseminate changes across the Council</p>	<p>IG strategy approved at April 2013 Cabinet.</p> <p>Corporate Information Security Policy currently under review – due for finalisation by end of May 2013.</p> <p>Other policies and procedures that form part of the security framework are in draft pending agreement by the SIRO following approval of the IG strategy in April 2013.</p>
4	Complete Corporate Retention & Disposal Schedule	Complete
5	Investigate instances of possible data breaches and ensure appropriate improvements within services and processes are made.	Ongoing
6	Support service areas during and after service reviews/restructures to address any information security risks that arise.	Ongoing
7	Support information sharing and the production of information sharing agreements	Ongoing
8	Monitor the publication scheme and ensure service areas are keeping it up to date	Ongoing
9	Review and update intranet and internet pages for FOI and DPA	Complete – intranet Planned completion end of May 13 for internet

No	Task	Completion Date & Comments
10	Complete N3 connection assessment for central government	Complete apart from awaiting confirmation from Connecting for Health on one requirement.
11	Support service areas in the completion of Privacy Impact Assessments for new systems/applications and those for priority existing applications	Ongoing
12	Rationalise IG file structure	Complete
13	Report to the Audit Committee on progress against the work programme and any issues arising	June 2012 - Complete September 2012 - Complete June 2013 – In progress