TELFORD & WREKIN COUNCIL

AUDIT COMMITTEE 27th JUNE 2017

J

INTERNAL AUDIT, INFORMATION GOVERNANCE & CALDICOTT GUARDIAN ANNUAL REPORT 2016/17

JOINT REPORT OF THE AUDIT & GOVERNANCE TEAM LEADER AND FAMILY CONNECT SERVICE DELIVERY MANAGER

1 PURPOSE

1.1 To present the 2016/17 Internal Audit, Information Governance (IG) & Caldicott Guardian Annual Report to the members of the Audit Committee and to seek their agreement to the 2017/18 IG Work Programme.

2 RECOMMENDATIONS

2.1 That members of the Audit Committee note the Internal Audit, Information Governance & Caldicott Guardian Annual Report for 2016/17.

2.2 That members of the Audit Committee agree the 2017/18 IG Work Programme.

3 SUMMARY

3.1 The terms of reference of the Audit Committee include:

1. "The approval (but not direction) of and monitoring of progress against, the Internal Audit Charter and Plan".

9. Consider the effectiveness of the Council's governance processes and their compliance with legislation and best practice including:

b) the Council's information security framework;
c) receipt of the Caldicott Guardian's Annual report;

This report presents information to meet the requirements of these sections of the terms of reference and to continue to demonstrate good governance and support the Annual Governance Statement (AGS).

3.2 The Public Sector Internal Audit Standards are deemed as proper practice under the Accounts and Audit Regulations 2015 for Local Government in England. The standards state:

2450 Overall Opinions

When an overall opinion is issued, it must take into account the expectations of senior management, the board and other stakeholders and must be supported by sufficient, reliable, relevant and useful information.

Public sector requirement

The chief audit executive must deliver an annual internal audit opinion and report that can be used by the organisation to inform its governance statement.

The annual internal audit opinion must conclude on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control.

The annual report must incorporate:

- the opinion;
- a summary of the work that supports the opinion; and
- a statement on conformance with the Public Sector Internal Audit Standards and the results of the quality assurance and improvement programme.

This report meets these requirements.

4 PREVIOUS MINUTES

Audit Committee 30th June 2015 – Internal Audit & Information Governance Annual Report and Quarter 4 Update report 2014/15
Audit Committee 15th September 2015 – Caldicott Guardian Annual Report 2014/15
Audit Committee 30th June 2016 – Annual Internal Audit, IG and Caldicott Guardian Annual Report 2015/16

5 2016/17 INTERNAL AUDIT ANNUAL REPORT

5.1 Assurance and Opinion

5.1.1 The Council's section 151 officer's statutory obligation under the Accounts and Audit Regulations 2015 to review the effectiveness of the system of internal control is informed by the work of Internal Audit. The assurance derived from this work 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 Council's framework of governance, risk management and internal control which is included within the Annual Governance Statement.

5.1.3 The planned Internal Audit resources for 2016/17 were 991 days plus 60 days (1051) specialist ICT audit provided by the framework contract. The planned resources were affected by the departure of the temporary auditor in August 2016 but were supplemented by further use of the framework contract and use of the Compliance Officer to undertake schools audits. The team achieved just under 90% of the planned work but several items have been rescheduled into 2017/18 due to delays in the introduction of new processes following restructures and the change in timetable for the implementation of various IT upgrades. The productive work of the team was also slightly affected by the preparations and support for the external assessment against the PSIAS (see section 5.2 of this report).

5.1.4 Based on the work undertaken during the year (areas attached as **Appendix A**) and the implementation by management of the agreed recommendations, Internal Audit's annual opinion provides reasonable assurance in respect to the adequacy and effectiveness of the Council's framework of governance, risk management and internal control within the areas of the Council reviewed during the year.

5.1.5 As in previous years Senior Management have provided information or updates to the Audit Committee where requested to provide explanations as to why progress on the implementation of recommendations was not as agreed.

5.1.6 As in previous years this Annual Report includes information in respect to the type and number of recommendations made during the year (as requested by the Committee). This information is shown below for 2016/17 with comparisons with 2015/16 and 2014/15 shown in brackets.

Number of Recommendations made by Type 2016/17 (2015/16 2014/15)

No. of Audit Reports & Grading	Total number of recommendations	Financial Regulation)	Legal	Policy and/or Procedure	Best Practice
71 (65 45) ***3 (7 2) Green*** ***50 (34 24) Yellow*** ***17 (18 13) Amber*** ***1 (2 4) Red***	**682 (726 541)**	**162 (147 68)**	**40 (48 20)**	**445 (484 430)**	**35 (56 23)**

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

5.1.7 71 audit reports were issued during 2016/17, 6 more than 2015/16. Out of the 71 reports 4% (11% 5%[1]) were green (good), 70% (56% 56%) were yellow (reasonable), 24% (30% 30%) were amber (limited) and 2% (3% 9%) were red (poor). The percentage for green reports has reduced and yellow increased. Amber and red grading have reduced in percentage terms but were actually only 1 less than 2015/16.

5.1.8 30% of the recommendations were legal/financial regulation compared to 27% in 2015/16 and 16% in 14/15. 65% of the recommendations were policy and procedure compared to 67% in 2015/16 and 79% in 14/15. These differences can be influenced by the areas reviewed during each audit year but again reflect the findings from previous years in that the impacts of reduced resources, restructures and change affect the understanding of controls and the importance of their application. In addition the audits have highlighted the importance of effective handover/succession planning, training and clear understanding of staff of their revised roles and responsibilities.

5.2 Public Sector Internal Audit Standards (PSIAS) and External Assessment

5.2.1 The Public Sector Internal Audit Standards (defined proper practice under the Accounts and Audit Regulations 2015) were effective from 1st April 2013 and in January 2017 there was an external assessment undertaken against the standards. This is a requirement that must occur every 5 years.

5.2.2 The assessor concluded - “I identified no areas of non-compliance with the standards that would affect the overall scope or operation of the internal audit activity”. However recommendations and suggestions were made and accepted by the team which are in the process of being implemented. An update on progress is shown in the quarter 4 update report also on this agenda and further updates will be provided to the Audit Committee during 2017/18.

[1] Figures in brackets are for 2015/16 and 2014/15

5.2.3 The Quality Assurance & Improvement Programme (QA&IP) was followed during the year and any actions have been fed back to the team, individuals or been used to update the teams processes.

5.2.4 As part of the standards it is a requirement to outline in the annual report where there is any non-compliance and these are referred to in the External Assessment report referred to in paragraph 5.2.2 and the Quarter 4 update report to this Committee. The CFO and Monitoring Officer are satisfied with the position in respect to the areas of non-compliance and action to be taken.

5.3 Performance reviewed by External Audit

5.3.1 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 2016/17 required by the External Audit and they have indicated that the work is of a good standard and that they can place reliance on it (although the working papers provided by our contractor were not as high standard as those provided by the team).

5.3.2 The External Auditor has used our external assessment against the Public Sector Internal Audit Standards to inform their reliance on our work. They were satisfied with the assessment and the actions being taken to address the recommendations made. No other issues have been raised.

5.4 Improvement Activity

5.4.1 During the year to improve the team's efficiency, effectiveness and productivity we have held team meetings and development sessions. In addition since the external assessment we have looked to make changes to improve our adherence to the Standards. Continually during the year we have investigated and implement new/alternative ways of service delivery (practices, use of technology, procedures and standard documentation) based on our analysis, customer feedback (see 5.5), sharing best practice with other local authorities and service providers.

5.4.2 The Audit, IG and Insurance SDM has continued to have links with CIPFA's Audit Panel despite the governance and future direction of the Panel being unclear since June 2016. This continues to help the team to develop and provides early awareness of developments in public sector Internal Audit and Governance. Other members of the team also attend regional Fraud, Contract and Unitary/Met Authority groups (when relevant) which assist in identifying best practice and different approaches to audit work and information exchange.

5.5 Customer Feedback

5.5.1 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

5.5.2 The analysis of post audit questionnaire feedback is shown in the table below compared to the last 2 years. The exceptionally high ratings of recent years have continued to improve further.

POST AUDIT QUESTIONNAIRE FEEDBACK 2016/17 compared to last 2 years

Question	2014/15 From top score 5	2015/16 From top score 5	2016/17 From top score of 5	Difference 15/16 to 16/17
Pre- Audit Arrangements	4.9	4.8	4.9	+ 0.1
Audit Visit	4.9	4.9	4.9	No change
Communication	4.8	4.8	4.6	- 0.2
Report	4.8	4.8	4.9	+ 0.1
Is audit a positive support – Yes	100%	100%	100%	No change

The team's customer performance has remained extremely high during 2016/17 with the average score being 4.6 or more. There is a 4% reduction in respect to the score for communication (although it remains high) which has been affected by management changes during audits but and we have also identified and addressed any improvements required to our processes. The maintenance of these scores is a credit to the team and how they have approached their work and the audit of many services during or just after a restructure.

6 2016/17 INFORMATION GOVERNANCE ANNUAL REPORT

6.1 There are a number of pieces of legislation and good practice standards that govern the IG arrangements of the Council and these are listed in the background information at the end of this report. The Information Commissioners Office (ICO) is the regulatory body responsible for ensuring Council's meet information legislative requirements.

6.2 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 for the period covered by this report was the Assistant Director: Governance, Procurement & Commissioning with the Audit, IG, Insurance & Investigation Service Delivery Manager designated as the Deputy SIRO.

Information Rights

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

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

6.4 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.

It also co-ordinates and guides service areas 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.

6.5 The ICO has previously set a benchmark of 80% for responding to FOI requests within the 20 working day statutory deadline for responding to requests. Recently the ICO has revised the benchmark to 90%, this will be used as the target for 2017/18.

6.6 See table below for figures relating to FOI performance for the year 1 April 2016 to end of March 2017 compared with the same period for the previous year:

	16/17	15/16	% Increase / Decrease
Number of FOI requests received	1226	1090	+12
Average number of FOI requests received per month	99	90	+10
% of FOI requests responded to within statutory deadline	88	81	+9
Average time taken (days) to respond to each request	11	14	-21

As can be seen from the figures in the table above, the Council's performance in responding to FOI requests within statutory deadlines improved (up by 9%) from 2015/16. This performance improvement was realised despite the IG Team not having an Apprentice for a 2 month period and an increase in the number of requests received.

In addition to the above the Council received 59 requests (148 in 15/16) that were processed under the Environmental Information Regulations (EIR) 2004. The decrease in the number of EIR requests received is mainly due to Public Protection re-classifying how certain requests were dealt with, i.e. they were dealt with as business as usual requests rather than EIR requests. 86% (93% in 15/16) of these requests were responded to within the 20 day deadline.

6.7 In this period IG have received and responded to 10 appeals from requestors who were not satisfied with the response they received to their FOI request. This compares to a total of 14 appeals in 2015/16.

6.8 During this period IG received 3 complaints/referrals from the Information Commissioner (ICO) in respect to complaints made to them by FOI/EIR requestors. See below for a summary of each case:

A) Case 1 – a requester made a complaint to the ICO regarding the Councils application of FOI exemptions. The ICO found in favour of the Council and stated that they believed the Council had correctly applied the relevant exemptions. The requester did not agree with the ICO's opinion and has therefore taken the matter to the First Tier Tribunal. The Council has not received a decision from the tribunal to date.

B) Case 2 - a requester made a complaint to the ICO regarding the Councils application of FOI exemptions. The ICO partially found in favour of the requester. The Council does not fully accept the findings of the ICO but will release further partial information to the requestor but plans to appeal to the First Tier Tribunal in respect to the remaining information.

C) Case 3 – a requester complained to the Council that they held inaccurate information about the requester on their systems and requested that the Council amend said information. The Council agreed to record the requester's views on the relevant Council records. The requester was still unhappy with this matter and made a referral to the ICO. The ICO stated that the Council had acted in accordance with good practice in their initial action but further evidence provided by the requester to the ICO meant that further action was required by the Council. This action has been implemented in full.

6.9 Between 1 April 2016 and 31 March 2017 the Council received 62 Subject Access Requests (SAR's), this compares to 55 requests for the same period in 2015/16. 89% of SAR's received have been processed within the 40 calendar day deadline (70% of SAR's processed within deadline for 2015/16). These statistics demonstrate a significant improvement in performance during 2016/17.

It should be noted that the size and complexity of subject access requests increases year on year. For the 62 requests responded to in 2016/17, the IG Team had to read and redact over 10,000 pages of mainly sensitive personal social care information. The largest individual request required 2,232 pages to be read and redacted as appropriate by IG officers. IG continually review its procedures for processing subject access requests and feel that these are streamlined and fit for purpose. However further reviews will take place to ensure processes improve where possible.

It should also be noted that the Council did not receive any complaints/referrals from the ICO during 2016/17 in respect to its processing of subject access requests.

6.10 The IG Team also supports schools (T&W schools and one out of area school) with their information rights requirements. This is a traded service to schools and during 2016/17 the Team has supported 17 schools in relation to information rights and generated over £3,000 worth of income.

Data Security Incidents

6.11 IG supports the investigation (with service areas) of 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 mobile phone to confidential/sensitive information being communicated to an unauthorised and/or incorrect recipient.

6.12 IG (with the assistance of service areas) investigated all reported incidents of possible data and has confirmed that 34 data breaches had occurred (25 data breaches were identified in 2015/16). 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	**31** (22 in 15/16)	**31**
Accidental release of personal information verbally	**0** (2 in 15/16)	**0**
Documents containing sensitive information left in an insecure location	**1** (1 in 15/16)	**1**

Information lost or stolen	**2** (0 in 15/16)	**0**
TOTAL	**34** (25 in 15/16)	**32**

**It should be noted that the majority of these were referrals and not corporate complaints*

Unfortunately there has been an increase (36%) in the number of confirmed data breaches in 16/17 (following drops of 43% in 15/16 and 50% in 14/15). It is suggested that the increase can be attributable to the Council handling a consistent or even increased number of pieces of personal data but with less staff to undertake secondary checks/quality assurance on outgoing correspondence. The IG Team continues to work with service areas to improve personal data handling/processing.

6.13 For each of the confirmed breaches IG agrees actions with the relevant management team to minimise the impact of the breach on the customer. The Council also reviews and changes procedures and provides targeted training to reduce the possibility of similar data breaches occurring in the future.

6.14 Any lessons learnt from data security incidents/breaches 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 April 2016 – September 2017 are attached as Appendix B for information.

6.15 None of the data breaches detailed above were serious enough to meet the Information Commissioner's rationale for reporting serious breaches to them.

6.16 Out of the 36 confirmed data breaches investigated, appropriate disciplinary action has/or will be taken in 2 cases. Disciplinary action will range from written warning to possible dismissal.

6.17 In January 2017 the Council voluntarily took part in a review of its data breach reporting arrangements undertaken by the ICO in preparation for the introduction of the General Data Protection Regulation in May 2018. Although a grading or formal opinion was not given by the ICO at the conclusion of their review they did provide informal feedback stating the Councils arrangements were 'pretty robust'. The ICO report cited 5 recommendations for the Council to consider. The IG Team accepted these recommendations and all 5 suggested improvements have been implemented in full.

Information Governance Work Programme

6.18 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 2016/17 IG work programme was agreed at the June 2016 Audit Committee. Progress to date in respect to this programme is shown attached as Appendix C.

6.19 Appendix D details the proposed IG work programme for 2017/18 for approval. This programme mainly incorporates key actions required to facilitate the legal requirements of the GDPR.

6.20 The next update to the Audit Committee on Information Governance will be the 2017/18 update report, incorporating activity during April – mid August 2017 which will be presented to the September Audit Committee.

Information Governance Related Audits

6.21 In 2016/17 the Internal Audit Annual Plan encompassed a review of the Council's Records Management arrangements. This audit commenced in 2016/17 but has not been finalised to date. An update on the status of this audit will be presented at the September Audit Committee.

6.22 Also in 2016/17 audit follow ups were undertaken on a number of previously completed audits in 2015/16. The status of these follow ups are detailed below:

Audit	Grading in 15/16	Grading in 16/17
Payment Card Industry Standards	Yellow – Reasonable	Green - Good
Information Sharing	Yellow – Reasonable	Green - Good
Information Security	Yellow – Reasonable	On-going (all IG actions complete, awaiting confirmation from ICT on their actions)

7 2016/17 CALDICOTT GUARDIAN ANNUAL REPORT

Caldicott Guardian (CG) Function – Key Responsibilities

7.1 A requirement for the Audit Committee to consider the Caldicott Guardians (CG) annual report / action plan. The first CG report was presented at the June 2015 Audit Committee meeting. An update on the progress made in completing the CG action plan can be found in Appendix E.

7.2 In August 2016 Richard Smith (previously AD: Early Help & Support and Caldicott Guardian) left the authority. Since this date Debbie Lloyd, (Family Connect Service Delivery Manager and previously Interim AD: Early Help & Support) has fulfilled the role of Caldicott Guardian. Sarah Dillon was appointed to the AD: Early Help & Support role in February 2017 and will be undertaking the CG training shortly.

8 Looking Forward

8.1 Currently each EU country has their own data protection laws which are a variation on the main European directive. In the UK we are currently governed by the Data Protection Act 1998. The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. The outcome of this reform is that from 25 May 2018 the UK will be bound by one single item of data protection legislation, the General Data Protection Regulations (GDPR).

8.2 The key changes this legislation will bring are:

- The number of data protection principles is reducing from 8 to 6 but broadly cover the same areas as the DPA 1998

- Parents or individuals with parental responsibility must give consent to 'information society services' such as social networking sites for any child under 16 (Member states can lower this threshold to a minimum of 13 years old)
- Data portability – an individual's right to have their personal information transferred to another data controller on their request
- An individual's 'Right to be Forgotten' – data controller, in some circumstances, must erase all personal data relating to an individual
- Mandatory requirement to report data breaches that match certain criteria (currently this is not a mandatory requirement under DPA 1998)
- Fines for data breaches can be a maximum of 4% of annual global turnover or 20 million Euros (not clear how this will affect the public sector as yet). Currently under DPA 1998 the maximum fine is £500,000
- Organisations meeting certain criteria will be required to have a statutory role of Data Protection Officer

8.3 The IG Team has devised a corporate action plan to help services ensure that the requirements of GDPR are implemented by 25 May 2018. In addition to this plan the IG Team are producing a set of guidance notes that will support services in reviewing their arrangements for processing personal data in line with GDPR requirements. To complement each guidance note, the Organisation Delivery & Development Team will be producing online training material that all officers will have access to.

9 CONCLUSIONS FOR 2016/17

9.1 Despite limited resources and changes to services during the year and therefore the rescheduling and re- defining of scopes the Internal Audit and Information Governance Teams have performed well and made a positive contribution to the governance arrangements within the Council.

9.2 The statutory responsibilities of the Council's Chief Financial Officer (section 151 officer) in respect to internal audit and internal control have been met and Internal Audit has provided reasonable assurance to the Council on the Council's internal controls, governance and risk management processes for the areas reviewed in 2016/17.

9.3 The Internal Audit and Information Governance Teams have also continued to provide advice and guidance on governance, procedures, controls, information security and risk management.

9.4 However, there are numerous major changes occurring both within and outside the Council during 2017/18 and beyond which could affect the team's activities e.g. :-

a) The continued pressure on the Council's budget strategy for 2017/18 and beyond, including the revised Audit & Governance structure that will be implemented in June 2017. The proposals should maintain the Internal Audit performance and they are designed to achieve the statutory requirements of Information rights legislation and ICO guidance;
b) Changes in any information rights legislation and guidance particularly the preparations for the General Data Protection Regulations (GDPR) which come fully into force in May 2018 (replacing the 1998 Data protection Act);
c) Further service restructures and re-engineering across the Council, 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) The Council will have a new external audit contract from April 2018 for the audit of the 2018/19 accounts which may mean new external auditors. (KPMG will complete the 2017/18 under the existing contract);

f) The revised Caldicott Guardian arrangements may continue to require additional support until they become more familiar with their role;

g) The Council's key projects including Adult Social Services, Children's Safeguarding, the commencement of the implementation of one IT system for adults and children's services, transferring services to other providers, introduction of a new HR/Payroll system during 2017/18 and developing further commercial activities.

10 OTHER CONSIDERATIONS

AREA	COMMENTS
Equal Opportunities	All members of the Internal Audit and Information Governance Teams 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 and Information Governance Teams are environmentally aware and if any issues were identified they would be notified to the appropriate manager.
Legal Implications	The Accounts and Audit Regulations 2015 sets out the detailed requirements for local authorities in relation to keeping adequate accounting records and control systems, preparing, approving and publishing a statement of accounts, and making various documents available for public inspection, and objection and questioning by local electors. The authority "must ensure" that it has (and reviews) a "sound system of internal control": Regulation 3. It "must undertake an effective internal audit": Regulation 5. There is a new requirement to prepare and publish a "narrative statement", commenting on the authority's financial performance and economy, efficiency and effectiveness in the use of resources over the year. The information set out in this report illustrates the work that has been undertaken to meet the appropriate statutory requirements. The Public Sector Internal Audit Standards (PSIAS) is mandatory across the whole of the public sector. The purpose of the PSIAS is defined as follows: • define the nature of internal auditing within the UK Public Sector; • set basic principles for carrying out Internal Audit in the UK Public Sector; • establish a framework for providing internal audit services in respect of organisational processes and operations; • facilitate the development of an effective Quality Assurance and Improvement Programme and; • define a mandatory Code of Ethics. Undertaking the audits as set out in the report, and providing updates and an Annual Report to this Committee contributes towards meeting these requirements.

	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 5.1.1, 6.1 and 6.3 respectively. 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. Compliance with the Information Rights legislation mentioned in this report at paragraph 6.3 is mandatory. When assessing compliance, the ICO will consider approved policies and procedures of the authority. Each NHS organisation is required to have a Caldicott Guardian under Health Service Circular HSC 1999/012 dated 22 January 1999. The Circular applies to all organisations which have access to patient records, including acute trusts, ambulance trusts, mental health trusts, primary care trusts, strategic health authorities, and special health authorities such as NHS Direct. Caldicott Guardians were subsequently introduced into social care with effect from 1 April 2002, under Local Authority Circular LAC (2002)2 dated 31 January 2002. Caldicott Guardians play a key role in ensuring that the NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information under a framework which complies with the requirements of the Data Protection Act 1998; they actively support work to enable information sharing where it is appropriate to share; and advise on options for lawful and ethical processing of information. NHS and Social Care Caldicott Guardians are required to be registered on the publicly available National Register of Caldicott Guardians. The UK Council of Caldicott Guardians, an elected body made up of Caldicott Guardians from health and social care, meets four times per year and has a published strategy, currently for 2011-2016. The Health & Social Care Information Centre [HSCIC] publishes guidance and resources for Caldicott Guardians. SD 19.04.2017
Links with Corporate Priorities	All aspects of the Audit and Information Governance teams work support good governance which underpins the achievement of the Council's objectives and priorities.
Risks and Opportunities	All aspects of the Audit and Information Governance teams work supports managers and the Council to identify and manage their 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	The service areas within the Internal Audit, Information Governance and Caldicott Guardian teams/roles operated within their budget allocation of £543k for 2016/17. The teams are undergoing a restructure with the proposals launched in April, the closing date for comments being 17th May and

	implementation being 12th June, with targeted savings expected to be met of £147k. The external audit fee was £122k in 2016/17 a reduction of £20k on what was expected. The implications for a data breach could result in fines of £500,000. No fines for data breaches have been levied in the period under review and the Council budget does not anticipate any such fines being levied. There are no financial implications anticipated from adopting the recommendation of this report. RP-20.4.17
Ward Implications	The work of the Audit & Information Governance teams encompasses all the Council's activities across the Borough and therefore it operates within all Council Wards.

11 BACKGROUND PAPERS

Annual Audit Plan 2016/17 and Charter
Public Sector Internal Audit Standards – Applying the IIA International Standards to the UK Public Sector 2013 and External Assessment January 2017
CIPFA Local Government Application Note - April 2013
Accounts and Audit Regulations 2015
Corporate Information Security Policy
Corporate Information Security Breach Procedure
Local Authority Data Handling guidelines
ISO27001 (standard for information security)
Data Protection Act 1998
Freedom of Information Act 2000 (fully introduced 2005)
Environmental Information Regulations 2004.
Caldicott Review - https://www.gov.uk/government/publications/the-information-governance-review
Information: To Share or not to Share – Government Response to the Caldicott Review.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Report by Jenny Marriott, Audit, IG, Insurance & Investigations SDM. Telephone: 383101
Rob Montgomery, Audit & Governance Team Leader. Telephone 383103
Debbie Lloyd, Family Connect SDM Telephone 388571

APPENDIX A

Work undertaken during 2016/17 to provide assurance and the Internal Audit Opinion

Audited areas	Days
AGS Certification Assurance 2015/16	12
Abraham Darby Leisure Centre	17
Additional Payment to Foster Carers	11
Adult Social Care Payments	1
Advice & Consultancy including org change	111
Apley Wood Primary	6
Aqueduct Primary	7
Arthog	18
Assistive Technology - Early help & Support	7
Bank contract review	1
Benefits 2016-17	16
CVS contract	1
Captain Webb School follow up	1
Cash Collection 2016-17	22
Catering - Commercial Nurseries	8
Children's Direct Payments follow up	1
Children in Care Savings	9
Children's arrangement orders	5
Children's Brokerage (Link to Foster Care)	4
Church Aston Primary School	5
Civica Upgrade	2
Community Support Finance Audit	9
Contract Waivers	1
Core Groups for Safeguarding	8
Corporate Leases (Including Nursery Schools)	12
Council Tax / NNDR 2016-17	33
Council Tax / NNDR 2017-18	1
Customer Contact Centre	7
Deferred Payments follow up	1
Donnington Wood Infants School	9
Early Intervention (Common Assessment Framework)	1
Employment Code of Practice Compliance	1
Events Management	4
Family Nurse Partnership	1
Follow ups - general	34
Fraud & Compliance Checks including NFI	16
GPC	8
General Ledger 2016-17	29
Health & Safety review	12
Home Education Process Review	1
Home from Hospital (Mental Health)	5
ICT Wireless Provision	1
Inter-agency communication in relation to missing children	1
John Fletcher of Madeley Primary School	7

Joint Commissioning & Information Sharing (Review of Processes	1
Leaver Checklist	1
Leisure - Central Admin processes	10
Lilleshall Primary School	8
Local transport grant	2
Madeley Parish Council	1
Making Safeguarding Personal (Adults)	7
Moorfield Primary School	7
My Choices	7
My Options	8
National Careers Service	1
Newdale School Follow Up	2
Newport Infants School	7
Nuplace	17
Oakengates Leisure Centre	10
Oakengates Town Council	2
PSE Upgrade project assurance	2
PSP Register (management of personal data)	6
Pride in the Community	6
Pride in the High Street & Monitoring	3
Process for developing, reviewing & monitoring SLAs & MOUs	2
Procurement Contract reviews	3
Property Investment Portfolio (Review of bad debts) follow up	1
Sales Ledger 2016-17	16
Section 106 Agreements	7
Section 17 payments follow up	1
Shortwood School	8
Sickness Monitoring review in Early Help & Support	7
Ski Centre 2016-17	8
Social Letting Agency follow up	2
Social Media Compliance Work	3
St Lawrence Primary School	8
St Matthews Follow up	1
St Patricks RC Primary School follow up	1
St Peters & Pauls	7
St Peters Edgmond	7
Supervision Policy Review (incl. Children's Safeguarding)	9
Support Planning Early Help & Support	8
Teagues Bridge Primary School	11
Telford Ice Rink - Vending Machines	3
Temporary Accommodation	6
The Bridge School	6
The Place - Follow up	2
Tibberton Primary School	8
Town Park - Follow ups	6
Transition Process children's to adults care	9
Transparency	2

Treasury 2016-17	11
Troubled Families Grant	3
West Rd / Granville House imprest account	2
Wombridge Follow Up	2
Wrekin View Primary School	7
Wrekin View Follow Up	2

APPENDIX B

Information Security Incidents: Lessons Learnt – 2016/17

Information Governance (IG) 1st Half Yearly Update – 1 April to 30 September 2016

Despite your vigilance and further training/publicity the Council has continued to experience data security incidents including some minor breaches during the first half of the year. Following investigation by service areas/the IG team changes to local processes have been agreed. However there are wider lessons to be learnt or reminders for us all from these incidents and this note aims to share them with you.

Top 3 reasons for incidents at Telford & Wrekin

1. Emails sent to incorrect recipients
2. Contact details not being updated on systems on a timely basis
3. Human error – typing errors, lack of checking contact details, etc.

Reminders/Lessons learnt from these incidents

- ✓ Always check who you are sending an email to against who you think you are emailing particularly when the email address auto-populates in Outlook. Also If you are sending an email to a group email address check all the officers in that group are authorised to receive it
- ✓ You can select to not use the Auto-Complete function in Outlook, or clear the current entries in the Auto-Complete function by (in Outlook); 1) Click File tab 2) Click Options 3) Click Mail 4) Under Send messages, select or clear the Use Auto-Complete to suggest names when typing in the 'To' check box.
- ✓ Always use the Council's Secure Communication System (SCS – look under 'S' on intranet) or GCSX to electronically send personal information **externally**
- ✓ Ensure you regularly check customer contact details held in your area and update them on a timely basis where necessary
- ✓ When sharing and sending personal information NEVER assume. Think what the impact could be of your assumption(s). All your decisions need to be based on fact.
- ✓ Be careful when using Social Media and do not post personal information about your work, i.e. about your work colleagues or customers
- ✓ 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 transposed to 28 by mistake. But this mistake can be picked up by checking.

#what happens when it all goes wrong???

If you think you need to hold personal information unsecured on a work device or a USB stick do you ever think of this?

BBC NEWS

LIVE BBC NEWS CHANNEL

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Market Data
Your Money
Economy
Companies
Politics
Health

Last Updated: Wednesday, 14 February 2007, 16:16 GMT

E-mail this to a friend Printable version

Nationwide fine for stolen laptop

The Nationwide Building Society has been fined £980,000 by the City watchdog over security breaches.

The fine follows the theft of a laptop from a Nationwide employee's home which contained confidential customer data.

Nationwide security procedures were found to have failed

Lifestyle › Health & Families › Health News

Brighton and Sussex University Hospitals NHS Trust fined over privacy breach

A hospital trust has been fined £325,000 after computer hard drives containing confidential information on thousands of patients were stolen.

When you dispose of work IT equipment or documents in an insecure way do you ever think of this?

When you click on a website link detailed in a work email from a sender that you have never heard of do you ever think of this? Never click on a link or an attachment on an email from an unknown source. Be safe and check first!


TalkTalk counts costs of cyber-attack

Hack in October cost £60m and led to loss of over 100,000 customers

TalkTalk customers were left fuming after a cyber-attack. Photograph: Andrew Milligan/PA

3 Key Messages to Staff

1	Some staff state breaches are caused because they are in a rush due to workloads – **5 minutes saved by rushing causes days' worth of work in investigating a data breach**
2	Some staff are not checking or updating customer contact details – **the most common reason for data breaches this year is the use of incorrect addresses**
3	The Council can currently be fined a maximum of £500,000 – **As of May 2018 this fine could increase to over £16 million pounds!**

Make sure your actions do not result in the Council being fined or disciplinary action being taken against you

Mistakes have consequences – protect personal information

we can help

- Contact the IG Team on 82537 or email IG@telford.gov.uk
- Visit the IG intranet page for advice and guidance

APPENDIX C

Information Governance (IG) Work Programme 2016/17- Position as at 31/03/17

No	Task	Completion date	Position as at end March 17
1	Administer FOI/EIR/DPA requests, appeals and associated correspondence from the ICO.	On-going	On-going
2	Continue the provision and promotion of additional services to schools within and outside the area to generate agreed income.	On-going	On-going
3	Keep the T&W commercial website up to date to support the above.	On-going	On-going
4	Investigate instances of possible data breaches and ensure appropriate improvements within services and processes are made.	On-going	On-going
5	Support service areas to address any information security risks that arise.	On-going	On-going
6	Support information sharing and the production of information sharing agreements.	On-going	On-going
7	Support service areas in the completion of Privacy Impact Assessments for new systems/applications and those for priority existing applications.	On-going	On-going
8	Review and promote the CISP	End of April 16	Review completed and CISP will be promoted by end of Sept.
9	Finalise and promote Information Asset Owner guidance	End of June 15	Complete
10	Agree and deliver an IG training and awareness programme.	Agree programme (with SIRO) – End May 16 Deliver programme throughout 16-17	Agreed On-going
11	Update compliance work programme and undertake activities	Agree programme (with SIRO) – End May 16 Deliver programme	Agreed On-going

		throughout 16-17	
12	Review the Councils privacy notice and update where necessary.	End of June 2016	Complete
13	Complete Ollie module for classification scheme and promote scheme and policy.	End of July 2016	Module completed. Policy completed Delay in implementation as Office 365 move may offer technology to complement requirement. Task moved to 17/18 IG Programme
14	Report to the Audit Committee on progress against the work programme and any issues arising.	September 2016 June 2017	Complete
15	Produce gap analysis for the General Data Protection Regulations.	November 2016	Complete
16	Investigate channel shift options including use of disclosure log, open data, publication scheme and other communications from IG	September 2016	Complete
17	Review the IG strategy, update and get approved.	End of October 2016	Strategy updated and will be presented for approval with ICT Strategy.
18	Review the need for public task statement. Example : https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=6&ved=0ahUKEwiElejE-abLAhVCTBQKHa2MArYQFgg5MAU&url=https%3A%2F%2Fwww.leicester.gov.uk%2Fmedia%2F180379%2Fpublic-task-statement-2015.pdf&usg=AFQjCNEURU1rVbH_f2bmY_kYyUbjeDDZSw	End of December 2016	Complete
19	Review current IG policies in place to include as a minimum data protection, records management, information security breach procedure and information sharing.	End of March 2017	Complete
20	Create outstanding policies from the IG security framework and disseminate changes across the Council.	End of March 2017	On-going. Task will be completed in line with GDPR requirements.

21	Complete N3 connection assessment for central government.	End of March 2017	Complete
22	Implement findings of the IG related audits	As required in each audit report	Complete

APPENDIX D

Information Governance (IG) Work/Compliance Programme 2017/18

No	Task	Target Completion date
1	Administer FOI/EIR/DPA requests, appeals and associated correspondence from the ICO.	On-going
2	Continue the provision and promotion of additional services to schools within and outside the area to generate agreed income.	On-going
3	Keep the T&W commercial website up to date to support the above.	On-going
4	Investigate instances of possible data breaches and ensure appropriate improvements within services and processes are made.	On-going
5	Support service areas to address any information security risks that arise.	On-going
6	Support information sharing/production of sharing agreements.	On-going
7	Support service areas in the completion of Privacy Impact Assessments for new systems/applications and those for priority existing applications.	On-going
8	GDPR Action Plan – implement IG actions and refresh plan.	On-going
9	Review arrangements on Information Asset Owners including Information Asset Registers.	End of July 17
10	Agree and deliver an IG training and awareness programme.	Agree programme (with SIRO) – End May 17 Deliver programme throughout 17-18
11	Review compliance with ICO Privacy Notices Code of Practice (for GDPR).	End of July 17
12	Review compliance with Privacy Impact Assessments Code of Practice (for GDPR).	End of August 2017
13	Report to the Audit Committee on progress against the work programme and any issues arising.	September 2017 June 2018
14	Review compliance with Subject Access Code of Practice (for GDPR)	End of November 2017
15	Implementation of classification scheme.	End of December 2017
16	Review compliance with the Anonymisation Code of Practice (for GDPR)	End of January 2018
17	Review compliance with Data Sharing Code of Practice (for GDPR)	End of March 2018
18	Review and update the Corporate Information Security Policy (CISP)	End of March 2018
19	Create outstanding policies from the IG security framework and disseminate changes across the Council.	End of March 2018

20	Complete N3 connection assessment for central government.	End of March 2018
21	Implement findings of the IG related audits	As required in each audit report

APPENDIX E

Updated Position of the Caldicott Guardian Action Plan

Recommendation	Target date	Lead	Actions/Progress
Caldicott Review related actions - () = Recommendations from Caldicott Review			
1. Examine our existing arrangements, and lead by example with our local partners to make it easier to share information (introduction)	Ongoing	CG	There is a local sharing arrangement in place with health partners. This is reviewed as and when required by the agreement.
2. Ensure that relevant personal confidential data is shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual (2)	Ongoing	CG	See above.
3. Seek advice from the ICO and refer to the HSCIC's Confidentiality Code of Practice for further advice on managing and reporting data breaches (5)	As required	CG	Process in place via IG Team which ensures compliance
4. Explain and apologise for every personal data breach, with appropriate action agreed to prevent recurrence (5)	As required	CG	Process in place via IG Team which ensures compliance
5. Clearly explain to patients and the public how the personal information we collect could be used in de-identified form for research, audit, public health and other purposes (7)	Review public information given by March 2016	CG	JB attended health economy meeting. Public Information in process of being updated for all partners.
6. Make clear what rights the individual has open to them, including any ability to actively dissent (7)	As per 5. above	CG	To be addressed as part of 5. above
7. Use the best practice contained in the HSCIC's Confidentiality Code of Practice when reviewing information governance practices to ensure that they adhere to the required standards (12)	March 2016	CG/SIRO	Best practice is recognised as using IG Toolkit for external verification of our practice, which we have in place.
8. Ensure that social care providers use the Information Governance Toolkit (12)	Embed within Procurement conditions – March 2016 Monitor through Contract compliance March 2017	CG	Discussed with Commissioners. Share with SPIC Checked CQC standards
9. Appoint a Caldicott Guardian or Caldicott lead with access to appropriate training and support (15)	**Completed.** CG appointed and registered with Social Services CG Register. CG	CG	However existing CG left on 31 January. Deputy CG has assumed CG role in the interim until new CG

	attended accredited CG training on 18 November 2014.		has been trained and registered on national CG Register.
10. Local authorities consider extending Caldicott Guardian arrangements to children's services (15)	**Completed.** Role across Adult & Children's services	CG	To be looked at as part of the implementation of combined children's and adults management information system.
11. Strengthen leadership on information governance (15)	**Completed.** Council has now established regular meetings between CG and SIRO and supporting officers within the Council to monitor progress. CG has met separately with counterparts in Shropshire Community Trust and T&W CCG. Discussions underway with wider health and social care economy about establishing a pan-Shropshire group.	CG	Ongoing.
12. Ensure that the information provided to inform citizens about how their information is used does not exclude disadvantaged groups (19)	As per 5. above	CG	To be addressed as part of 5. above
13. Use the revised Caldicott principles in all relevant information governance material and communications (25)	As per 5. above	CG	To be addressed as part of 5. above
14. Investigate, manage, report and publish personal data breaches and ensure that commissioned bodies are investigated, managed, reported and published appropriately (6)	Ongoing	CG	Process in place via IG Team which ensures compliance
15. Implement appropriate arrangements in relation to information governance including the demonstration of strong leadership on information governance and adopt information governance procedures that are equivalent to those already established by healthcare providers (12)	March 2016	CG	This work is ongoing.

Other actions			
16. Share annual report with Audit Committee annually in June and an annual update in September.	Completed	CG	Ongoing
17. Address HSCIC recommendations arising from Information Governance Toolkit submission.	Ahead of next submission	CG	Awaiting the outcome of the 16/17 toolkit submission and associated recommendations to be made.
18. Complete register of Information Sharing Agreements and ensure reviews are held within agreed timescales.	December 2015	CG	Register is in place.
19. Review Use of Fax Policies	December 2015	CG	Our Corporate Information Security Policy is reviewed annually, including the guidance on use of fax machines.
20 Ensure IG training has been undertaken by all relevant staff	March 2016	CG	An IG training module is available on Ollie and forms part of the induction process for all officers. A revised module has been released in 2016/17. In addition to the above module officers are required, every 90 days, to answer 5 randomly generated questions based on the requirements of the Councils Corporate Information Security Policy (CISP).