Herefordshire Council

MEETING:	**AUDIT & GOVERNANCE COMMITTEE**
MEETING DATE:	**5 JULY 2013**
TITLE OF REPORT:	**INTERNAL AUDIT 2012-13 DATA PROTECTION 1998 – FORMAL WRITTEN RESPONSE**
REPORT BY:	**KNOWLEDGE AND INFORMATION SERVICES MANAGER**

1. Classification

Open.

2. Key Decision

This is not a key decision.

3. Wards Affected

None.

4. Purpose

The purpose of this report is to update Members formally on the actions and improvement undertaken, and those proposed to be undertaken, by the Knowledge and Information Service in response to the KPMG internal audit report dated 26th April 2013. Also to update Members formally on the initial findings of the Information Commissioner's Office consensual data protection audit 30th April – 2nd May 2013.

5. Recommendations

THAT:

(a) Subject to any comments the Audit and Governance Committee wishes to make, the report be noted; and

(b) The Committee supports and endorses the actions proposed in order to address the recommendations of the KPMG internal audit with respect to the Data Protection Act 1998; and

(c) The Committee supports and endorses the actions proposed in order to address the areas of improvement identified in the second draft of the ICO consensual audit with respect to the Data Protection Act 1998.

6. Alternative Options

6.1 There are no alternative options.

7. Reasons for Recommendations

7.1 The Audit and Governance Committee should be aware of the improvements made already and to maintain an overview of actions required to raise the corporate assurance level in relation to the implementation of the Data Protection 1998 act within Herefordshire Council, thus protecting the organisation from reputational damage, and statutory intervention and penalties from the Information Commissioners Office (ICO).

8. Key Considerations

8.1 This report addresses the request from the Audit and Governance Committee for a written response to the initial presentation by KPMG of their audit report findings, following an internal audit on Data Protection compliance undertaken as part of Herefordshire Council's internal audit plan for 2012/13. It also gives context to the findings and remedial action already undertaken or planned, including the initial findings of the external consensual audit on Data Protection undertaken by the Information Commissioners Office (ICO – currently at 2nd draft stage). Both reports have provided a rating of Limited Assurance but recognise the quality of the work already undertaken by the newly formed Information Governance team in 2012/13, and the work planned for 2013/14, to deliver the appropriate level of assurance. All IG/IS remedial activity is managed through the Information Security Risk Treatment Plan and reported to the IM&T Board and Steering Groups.

8.2 Summary of progress against the recommendations of the internal audit report Data Protection 1998 (Ref 67 /2012-13).

8.3 **KPMG Recommendation (1) – Personal data audit (Principles 1 - 2, 4 – 5)**

8.4 The Council should carry out personal data audits across its service areas as soon as possible. The results of the audit will assist the Council in compiling accurate Data Protection registration renewals with the ICO in April 2013.

8.5 **Actions (1)** – 79 team units out of 120 identified have now undergone an information inventory. The initial information asset register has been compiled ready for the next stage of work to map to service functions, information asset owners and administrators for September 2013, with training in place by December 2013 (an activity recommended by the ICO auditors).

8.6 Following September 2013 Information asset owners will be asked to complete a personal data template, including personal financial data, to address both the personal data audit requirements and to assess organisational risk in relation to card data and the PCI:DSS requirements. This will be undertaken in a phased approach to manage the impact on stretched services.

8.7 The Information asset register will include the systems where the data is stored, sharing a common reference with the ICT asset register being compiled by Hoople which will also support business continuity management.

8.8 In addition to the audits we may also need to amend our data registration entries to cover changes to processing of Electoral Information Register data to meet National Fraud Initiative requests to use the data. Worcestershire have raised this as a risk and we are awaiting the decision from the ICO.

8.9 Our Privacy Impact Assessments will be cross referenced with the register in order to verify personal data usage by systems and to tie into the ICT asset register. The templates and guidance are in now in use and published on the intranet.

8.10 **KPMG Recommendation (2) – Security breach incidents (Principle 7)**

8.11 Council staff should complete annual training on data protection and the safe processing of personally identifiable information. All staff should be made aware of the implications of personal data security breaches.

Furthermore, all staff should be aware of the internal procedures to identify and report security breaches. Any personal data security breaches should be reported to the senior management team as a matter of urgency.

8.12 **Actions (2)** – 80 Data Protection incidents have been logged since June 2012, 3 self-reported to the ICO and 3 further open incidents are likely to be self-reported. The ICO auditors have commented that the level of reporting is encouraging and reflects the high visibility of the new Information Governance Team. They have suggested that we also record near misses.

8.13 Changes to the NHS IG toolkit v 11 published in June include the mandatory reporting of Adult Social Care IG incidents assessed at Level 2 through the IG toolkit. We are reviewing our updated incident reporting procedures in the light of this new requirement to include the categorisation guidance as part of our general management of Data Protection incidents. This includes the role of the Council's Caldicott Guardian in the internal reporting of incidents.

8.14 Training has not yet been rolled out as there remain outstanding issues with the eLearning platform which Hoople are working to resolve. However all the Information Governance modules are ready to use as soon as those issues are addressed and a go-live date confirmed.

8.15 Specialist training was organised on four dates for Social Care teams and a three year training plan for bespoke training to teams to complement the generic mandatory training is being put in place. The teams identified as priorities for the next 12 months are Adult Social Care, Public Health and Child Social Care. In particular support for the section 75 staff coming back into the Council from WVT is required to bring them up to speed with the updated policy suite, guidance and procedures.

8.16 The Information Governance team has worked closely with HR to align Information Governance policies and procedures and combine links on the intranet to providebetter support to mobile staff e.g. working at home or in the field. In addition IG clauses have been included in the new staff contract.

8.17 **Recommendation (3) – Downloading sensitive and confidential data (Principle 7)**

8.18

- Device management software should be installed on all terminals at the Council, including laptops, to only allow authorised encrypted memory devices to be used. Device management software selected by the Council should include proactive monitoring controls such as the creation of automated email alerts, should an unauthorised external device be connected to the Council's network.
- Management should review available restrictions to prevent users from downloading personal and sensitive information when accessing their Council profile on non-authorised Council devices. This includes personal home computers and hand held devices.

All changes to policies, procedures and controls related to downloading sensitive and confidential data should be communicated to all staff in a timely manner.

8.19 **Actions (3)** – These risks are recorded on the Information Security Risk Treatment Plan which is used to manage and report information risks to the Knowledge and Information Steering Group, the IM&T Steering Group and the IM&T Board.

8.20 Switching remote desktop printing on for Members has enabled this for all staff with a compatible desktop. Hoople are looking at a solution to switch this capability off for staff but still enable Members to use this feature. The target date for implementation of this solution is July 2013.

8.21 The hardening of servers and mobile devices to prevent non-corporate devices being connected through USB ports is a key requirement that Hoople is investigating on behalf of the Council.

8.22 The media devices policy has been replaced by a Removable Media Policy which is compliant with the new Public Sector Network requirements. In addition work is progressing on a Mobile Device strategy supported by a technical options paper from Hoople and user stories from a workshop held on 7th June. The draft strategy will be presented to the IM&T Board in July.

8.23 **Recommendation (4) – Communication of Data Protection Act issues (Principle 7)**

8.24 A Data Protection Liaison should be assigned for each Council directorate. The Data Protection Liaison role should include the following:

- Ensuring the Data Protection Officer was aware of Directorate level working practices relating to personally identifiable data, and any changes which have occurred
- Communicating security breaches and data subject access requests to the Data Protection Officer.

8.25 **Actions (4)** – Since the KPMG audit the Knowledge and Information Steering Group (KISG) directorate Information Governance representation has become more established so that the work of the IG representation supporting People's Services and level of awareness of the staff was positively noted by the ICO auditors. The IG team are continuing to develop the relationship with management teams and representatives e.g. the Public Health team now have representation on the KISG.

8.25 The on-going restructure of Corporate Services is proposing to create an Access to Information unit to replace the Customer Insight Unit by December 2013 which will improve procedures and resilience around the Subject Access Requests and Freedom of Information processes in particular and address overlaps in complaints and data protection breach procedures involving members of the public.

8.27 **Recommendation (5) – Data Protection Act consent to process clauses (Principle 1 - 2)**

8.28 A review of all personal data collection forms used throughout the Council should be carried out. Any forms which do not comply with the Data Protection Act 1998 should have relevant Data Protection consent clauses inserted.

8.29 **Actions (5)** – Forms for collecting personal data are being identified as part of the information inventory of teams. In completing the information asset register, copies of privacy notices and forms used to collect personal data will be required. This activity will be followed through post September 2013 once the information asset owners have been identified as it is their responsibility to ensure these are fit for purpose. The Information Governance team will then seek assurance through appropriate sampling.

8.30 **Information Commissioners Office (ICO) draft findings**

8.31 Summary of areas for improvement identified in the 2nd draft of the ICO consensual audit in April/May focused on two specific areas: training and awareness; and records management. There are five key areas of improvement contained in the draft report which are consistent with the findings of the KPMG audit and a total of 42 recommendations. The five areas and comments are as follows:

8.32 **ICO Key area (1) – Information Asset Register**

8.33 The Council should develop a comprehensive Information Asset Register, supported by a network of Information Asset Owners, to provide a means of ensuring all personal data is accounted for and monitored for compliance with the DPA. This Register should link with the Council's risk registers and retention schedule.

8.34 **Actions (1)** – This is covered by the actions identified for KPMG recommendation (1) with the addition of the creation of a register of retention schedules to provide a cross reference to the items in the information assets register.

8.35 **ICO Key area (2) – Access control**

8.36 User access permissions should be reviewed regularly to ensure that access to personal data is restricted to those staff with a business need and to provide assurance that access permissions are being disabled or amended, as appropriate, when an individual leaves the organisation or moves roles.

8.37 **Actions (2)** - We have agreed a new IT access control policy which requires managers to review access permissions to the information they are responsible for every 6 months, with guidance of how to do this. This will be audited by the IG team and is part of the process improvement work to be delivered by October 2013 through the Employee Lifecycle project around starters and leavers

8.38 **ICO Key area (3) - Training**

8.39 Procedures should be developed to monitor completion of information governance training and to follow-up instances when induction training is not received or mandatory/refresher training is not completed in a timely manner.

8.40 **Actions (3)** - Training needs to be rolled out and the reporting established. The IG team will receive a report in the first week of every month to go to the KISG and inform any actions/ recommendations for improvement and usage. It will be part of a standing agenda item on training. The reports will also be included in the bi-monthly analysis to the IM&T Board.

8.41 **ICO Key area (4) – Agency and Temporary Staff**

8.42 The Council should ensure that all temporary staff receive at least a basic level of training in data protection and information security.

8.43 **Actions (4)** – Discussions are in progress with Hoople to determine approach. Hoople work with 9 other agencies as second tier suppliers so the challenge is how to achieve a reliable process across these agencies. The onus will be on the recruiting manager that they have evidenced the training has been completed and on Hoople that the mandatory Information Governance modules are completed before computer accounts are set up.

8.44 **ICO Key area (5) - Complementary specialist training**

8.45 The Council should complement the recently developed information governance training by developing bespoke, specialist training for staff in key roles and for higher-risk staff who are responsible for handling significant volumes of personal data and/or sensitive personal data.

8.46 **Actions (5)** – This will be covered by the actions identified for KPMG recommendation (2).

9. Community Impact

9.1 The Information Commissioners Office can exercise statutory powers to enforce compliance with the Data Protection Act 1998, impose fines of up to £500,000 for breaches of the act, or choose to prosecute individuals for offences under the act.

10. Equality and Human Rights

The report does not impact upon this area.

11. Financial Implications

11.1 Not acting on these recommendations increases the likelihood of large financial penalties for any data breaches reported to the ICO.

12. Legal Implications

12.1 Failure to deliver the actions places the Council at risk of further action from the ICO.

13. Risk Management

13.1 Until the Information Governance team can complete their 'Managing Information Safely' delivery plan the legacy practices, which have led both audits to issue the Council with a Limited Assurance grading, remain. Therefore the risk of failing to meet the requirements of the Data Protection Act 1998 is to be noted in the Corporate Services Risk Register with the reference RSK.PPP.049 until such time as the Council's 'managing information safely' delivery plan has been formally noted and agreed as delivered by the appropriate body or person.

14. Consultees

14.1 None.

15. Appendices

15.1 None.

16. Background Papers

16.1 None identified.

Further information on the subject of this Report is available from
Ellen Pawley, Knowledge and Information Service Manager on Tel 07792 880345