HAMPSHIRE COUNTY COUNCIL

Report

Committee/Panel:	Audit Committee
Date:	25 June 2015
Title:	Data Protection and Information Handling
Reference:	6719
Report From:	Director of Policy and Governance – Corporate Services

Contact name: Peter Andrews – Corporate Risk Manager

Tel: **01962 847309** **Email:** peter.andrews@hants.gov.uk

1. Summary

1.1. The purpose of this paper is to outline the governance arrangements the County Council has in place to ensure that the information in its care is appropriately safeguarded.

1.2. The Council has a legal and moral obligation to its customers, service users, citizens, employees, partners and other stakeholders to safeguard the personal and/or sensitive personal information it holds, processes or manages. It is obliged, under the terms of the Data Protection Act 1998, to ensure that all personal and sensitive personal information is protected from loss, destruction or unauthorised disclosure.

1.3. The Council has a range of processes, policies and systems in place to safeguard the information it holds and ensures that its staff are aware of their responsibilities through training. The Councils Digital Strategy is predicated on its ability to use the data it holds more effectively. The ability to share data with other organisations, safely and proportionately; and in compliance with the law is the key to delivering joined up services.

2. Contextual information

2.1. In December 2013 the LGA and Information Commissioners Office (ICO) jointly wrote to the Leaders of all English Councils expressing their concern that Local Authorities were subject to more reported breaches of the Data Protection Act than other areas of the public and private sectors, and encouraging Councils to take steps to improve the ways that they handled the sensitive personal information they held and used.

2.2. At the same time, the ICO released a Checklist for Local Authorities containing a series of questions that elected members and senior managers were encouraged to ask. A copy of this checklist, including the answers relating to Hampshire County Council is appended to this report as Appendix 1.

Since autumn 2010, when the ICO gained the ability to levy fines for data protection breaches, Local Authorities have represented around 37% of all the

fines levied, around £2.3 million. Although the County Council has experienced fewer incidents than other Authorities and has not been subject to any such fines, it is taking steps to increase its resilience against data security incidents.

Safe Information Handling

2.3. The loss of data not only exposes the County Council to the possibility of regulatory action or fines, but can also have significant effects on the relationships between some of the most vulnerable clients, their families and their relationship with County Council staff. Although the County Council maintains robust IT security to protect itself from cyber attacks, the main causes of data protection breaches are not IT system or security failures, but failures in the way that people handle electronic and paper based documents in simple work tasks.

2.4. Since 2011 the County Council has self-reported 8 data protection breaches to the Information Commissioner. 4 of those cases are currently under investigation. The ICO has chosen not to take any regulatory action against the County Council in the other cases, recognising that the County Council has good processes in place and has taken appropriate steps to ensure that incidents could not reoccur.

2.5. The County Council has taken steps to increase its resilience by adopting a Safe Information Handling Policy. This has been put together to provide staff with clear principles for handling information safely, and clear practical guidelines in what to do in the most common areas where data protection incidents can happen. The Policy stresses the responsibility of individual members of staff to make a judgement call on how sensitive a piece of information is, and to take a risk based approach so that sensitive information is not released inappropriately. It is supported by the County Council's disciplinary process.

2.6. The guidance document provides practical examples, based on the areas of previous data breach concerns and the demands of greater information sharing, to help staff make those judgements. It outlines the practical steps for keeping all sensitive information safe. This primarily means personal and sensitive personal information about our clients, customers and staff, but also includes information that is commercially sensitive to the County Council. A copy of the summary of this document is appended to this report as Appendix 2.

2.7. To support the introduction of the Policy and guidance, the County Council has launched a programme of awareness raising and training across the County Council. A new e-learning package was implemented in April 2015 and in the first 2 weeks of its launch over 2,300 staff undertook the training.

3. Information Risk

3.1. The County Council has an ever increasing dependency on accessing, using and sharing the information stored within its IT systems and therefore there is a clear need to ensure that it addresses the risks facing those information assets. This is a complex area, and one that crosses traditional service boundaries. The need for co-ordination, streamlining and awareness-raising is clear and therefore responsibility for information governance matters has been included into the remit of the Risk Management Board, which will ensure that a consistent and coordinated response will occur across the County Council.

3.2. One of the key aspects of the Government's Security Policy Framework, and thereby the expectations of central Government, health service and other partners, is that the Council has identified a senior executive who is accountable and responsible for information risk across the County Council.

3.3. The role is known as the Senior Information Risk Officer or SIRO, and has responsibility for the leadership of the Council's information governance arrangements, ensuring that identified information threats and vulnerabilities are followed up for risk mitigation and advising the Corporate Management Team on the level of Information Risk Management performance within the County Council, including potential cost reductions and process improvements.

3.4. The Director of Policy and Governance, who is also the chairman of the Risk Management Board, has been identified as the County Councils SIRO. In addition, similar responsibilities at departmental level have been identified and senior managers nominated to co-ordinate actions taken by each Department.

4. Data Sharing

4.1. Although the Data Protection Act is designed to protect the personal information of individuals, it can seem odd to members of the public why they have to answer the same questions to different public bodies, and often, different parts of the same public body. This is particularly the case in areas where medical and social care, overlap.

4.2. The County Council has formal data sharing agreements with its partners where joint services are being provided. These outline what information can be shared, under what circumstances and why. These are backed up with privacy assessments that outline the impacts to individuals of sharing particular personal information. These are in line with the guidance issued by the Information Commissioner's Office.

4.3. The County Council can share personal information when an individual gives consent for it to be used in a particular way. The County Council uses consent forms in many of its service areas. In addition, there are service areas where particular legislation allows the County Council to share personal information for particular purposes. An example of this is in the Trouble Families area. However, these individual regulations and legislation are complex and can be inconsistent.

4.4. This complexity in the ability for public bodies to share the personal information they hold with other public bodies to further broader social aims is recognised as a potential barrier to new digital based service delivery models, preventing data sharing across and within public agencies.

4.5. In March 2015, following on from the report from the Public Service Transformation Network, *Bolder, Braver and Better,* the Cabinet Office published the results of policy discussions that it had held with civil society organisations, privacy groups and representatives of the wider public sector. These recommended a permissive power for defined public agencies to share data for the purposes of improving the delivery or targeting of public services in specified areas of social policy. This was summarised by the notion of "reprocessing data for public good."

4.6. The County Council is working to ensure that its processes support this approach and are prepared in advance of any secondary legislation, which it is hoped will be introduced shortly.

5. Recommendation

5.1. That the Audit Committee notes the content of this report.

CORPORATE OR LEGAL INFORMATION:

Links to the Corporate Strategy

Hampshire safer and more secure for all:	yes
Corporate Improvement plan link number (if appropriate):	
Maximising well-being:	yes
Corporate Improvement plan link number (if appropriate):	
Enhancing our quality of place:	no
Corporate Improvement plan link number (if appropriate):	

Other Significant Links

Links to previous Member decisions:		
Title	Reference	Date
Direct links to specific legislation or Government Directives		
Title		Date

Section 100 D - Local Government Act 1972 - background documents

The following documents discuss facts or matters on which this report, or an important part of it, is based and have been relied upon to a material extent in the preparation of this report. (NB: the list excludes published works and any documents which disclose exempt or confidential information as defined in the Act.)

Document	Location
None	

IMPACT ASSESSMENTS:

1. Equality Duty

1.1. The County Council has a duty under Section 149 of the Equality Act 2010 ('the Act') to have due regard in the exercise of its functions to the need to:

- Eliminate discrimination, harassment and victimisation and any other conduct prohibited under the Act;
- Advance equality of opportunity between persons who share a relevant protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, gender and sexual orientation) and those who do not share it;
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Due regard in this context involves having due regard in particular to:

a) The need to remove or minimise disadvantages suffered by persons sharing a relevant characteristic connected to that characteristic;

b) Take steps to meet the needs of persons sharing a relevant protected characteristic different from the needs of persons who do not share it;

c) Encourage persons sharing a relevant protected characteristic to participate in public life or in any other activity which participation by such persons is disproportionally low.

1.2. **Equalities Impact Assessment:**

1.1. Race and equality impact assessment has been considered in the development of this report and no adverse impact has been identified

2. Impact on Crime and Disorder:

2.1. The activities reported within this report have no effect on crime and disorder.

3. Climate Change:

a) How does what is being proposed impact on our carbon footprint / energy consumption?

The activities reported within this report have no effect on climate change.

b) How does what is being proposed consider the need to adapt to climate change, and be resilient to its longer term impacts?

The activities reported within this report have no effect on climate change.

Data protection

Local authority information sharing and data protection checklist

Some key questions for leaders and senior managers:

- *Who is the officer responsible for information governance and are they aware of their responsibilities?*
  This is the Director of Policy and Governance, who is the County Council's nominated Senior Information Risk Officer, and chairman of the Risk Management Board
- *Do you have a Cabinet Member with lead responsibility for Data Protection Act (DPA) compliance*?
  This is included in the responsibilities of the Executive Member for Policy and Resources
- *Is your authority registered with the ICO as required by the DPA?*
  Yes
- *What transparency arrangements do we have in place for releasing and publishing information to the public?*
  The Council proactively publishes data and information that it holds on its website (http://www3.hants.gov.uk/opendata/) in accordance with the Council's Open Data Policy .
- *What procedures do we have in place for keeping data secure?*
  The Council has robust IT security arrangements and meets the ISO 27001 accreditation. The County Council meets the Information Assurance standards outlined in the Public Service Network Code of Practice Code of Connection, This certification involves an internal audit and a health check from an external security company. In addition, the Council has a range of policies and procedures at operational level across services. These are summarised in its Safe Information Handling Guide
- *What information governance arrangement do we have in place for sharing information, and for exchanging it securely when appropriate, with partners?*
  The Council publishes Data Sharing advice on its internal website, these are based on guidance published by the Information Commissioner. The County Council has formal data sharing agreements in place with its partners.
- *What procedures do we have in place for responding to freedom of information, information sharing and data protection subject access requests?*
  All requests are channelled through a central point of contact, with responses co-ordinated by individual service Departments

- *What are the risks to the authority with regard to data and how are they being addressed?*
  The County Council's risk registers are co-ordinated by the Risk Management Board. Disaster Recovery plans for IT are in place through a reciprocal agreement with Dorset County Council.
- *Is our information managed efficiently or can we make improvements?*
  The County Council constantly assesses the best ways to use the information it holds. This is being co-ordinated through the Council's Digital Strategy
- *What training do we give members and officers on data protection and information sharing and how do we ensure that knowledge is kept up to date?*
  All new Members are subject to an induction that includes consideration of Data Protection. A simple and straightforward electronic learning package, an Introduction to Data Protection, is available to all Members and staff. Additional training is provided to specific service areas.

Security

- *As part of training, are the workforce made aware of the importance of checking that only relevant information is sent to the right recipient, and that robust processes are in place to confirm that it has been received?*
  Yes, this is included in an Introduction to Data Protection
- *When transporting sensitive personal information, either electronic or paper, is it securely held?*
  Guidance on safe transportation of sensitive information is included in the Safe Information Handling Guide. Locked cases are used in areas of high sensitivity.
- *Is encryption used to protect personal information? Particularly when it applies to removable storage devices eg usb sticks.*
  Yes, encrypted data sticks and laptops are available and supplied to staff.
- *Are relevant employees aware to carry out identity checks before giving out personal information over the telephone? Some people will try and trick them out of information over the phone.*
  Yes, this is included in training.
- *Are they made aware that only a limited amount of personal data should be given out over the phone and that written confirmation might be necessary?*
  Yes, this is included in training.
- *Is confidential waste, either electronic or paper, securely disposed of? Failure to comply with this is a major cause of enforcement notices under the DPA.*
  Yes.

Managing personal information

- *Do your employees know to only collect the personal information they need for a specific business purpose?*
  Yes, this is included in training and embedded in work processes.
- *Is the requirement to tell individuals about new or changed business purposes understood?*
  Yes, this is included in training.
- *Is importance given to keeping information accurate and up to date?*
  Yes, this is included in training and embedded in work processes.
- *Is personal information that is no longer required securely disposed of according to data retention rules?*

  Yes, the Council has suitable Retention Policies in place.

Safe Information Handling - Your responsibilities as an employee

- As an employee, you are personally responsible at all times for the personal information in your care.
- You must safeguard its security whatever format it is in (paper or electronic) and wherever you are working (working at your desk, on site, from home, remotely or travelling). This includes diaries, briefcases, notebooks and mobile phones etc.
- You can be disciplined for not complying with the Act and HCC policies.
- The Information Commissioner Office (ICO) has the powers to issue fines of up to £500,000 and prison sentences, if you knowingly misuse or lose personal information.
- More information is in the Safe Information Handling Policy.

Data Security Common Sense Do's & Don'ts

- Lock any papers containing personal information away securely
- Use appropriate levels of security when setting up Hantsfile documents.
- Wear your ID badge when in HCC buildings and offer to assist people who are not wearing one.
- Take particular care when posting personal information to ensure it is sent to the right person – check, check & check again.
- Check email addresses are correct before pressing the send button.
- Keep personal information in locked cases whilst travelling.
- Destroy personal information when it is no longer needed and in accordance with the relevant Retention Policy.
- Ensure you read and understand Safe Information Handling Policy

- Don't give anyone your password or let them use your log-in (IT Helpdesk will never ask for your password)
- Don't put personal information or attach documents containing personal information into your Outlook Calendar – use the "mark private" button
- Don't release personal information to other organisations (including the Police) unless through an authorised process or sharing agreement.
- Don't use faxes to send personal information unless there is no alternative, and then only after checking the intended number first.
- Don't keep personal data on unencrypted computers or memory sticks.