By: Gary Cooke - Cabinet Member Corporate and Democratic Services
Amanda Beer – Corporate Director Engagement Organisation Design and Development

To: Policy and Resources Cabinet Committee

Date: 24 May 2016

Subject: Information Governance and Mandatory Training

Classification: Unrestricted

Summary: This paper reports on information governance in KCC and the training provided to all staff in this area.

1. INTRODUCTION

1.1 Kent County Council has a robust framework in place to manage information governance. This brings together all the requirements, standards and best practice that apply to the handling of information to ensure compliance with the law, including The Data Protection Act 1998 (DPA), Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR). The framework is designed to assist with the application of rules concerning confidentiality, privacy, data security, consent, disclosure and access to records.

1.2 The aims of the Information Governance Management Framework are to:

- Comply with Data Protection, Freedom of Information and related legislation.
- Respect individual's rights to privacy and confidentiality.
- Appropriately protect and secure information.
- Maintain accurate records.
- Use information to improve efficiency and enhance service delivery.

This is achieved by:

- Management accountability through designated roles and responsibilities – see Appendix 1.
- A comprehensive policy framework supported where appropriate by strategies and improvement plans – see the Information Governance (IG) portal on Knet http://knet/ourcouncil/Pages/information-governance.aspx
- The Cross-Directorate Information Governance Group providing support to the council's Senior Information Risk Owner and promoting good information governance.

- Information Asset Owners (IAOs), with the support of their Information Asset Administrators, ensuring that information risks are appropriately controlled in their service areas.
- Comprehensive guidance, training and support to managers and employees. Completion of two e-learning modules - Information Governance and Data Protection, have been mandatory for all employees since July 2013 and July 2015 respectively, following criticism from both the Information Commissioner's Office and KCC Auditors who identified that insufficient training was a key contributor in failures to comply with the Freedom of Information Act 2000 and the Data Protection Act 1998.

1.3 The **Senior Information Risk Owner** (the Director of Governance and Law/General Counsel) is KCC's senior responsible officer for Data Protection and Freedom of Information. The SIRO understands the strategic aims of the council and how these may be impacted by information risks. The other roles with primary responsibility for Information Governance are described at Appendix 1.

1.4 KCC has a cross directorate **Information Governance Group**, chaired by the SIRO, which meets quarterly. There are representatives from all areas of all four KCC Directorates. The principal purpose of this group is to support the SIRO by:

- Promoting good corporate information governance.
- Supporting the SIRO on information risk and compliance issues
- Representing divisional issues, concerns and achievements
- Developing and reviewing information governance policies.
- Monitoring information and records management policy and practice.
- Monitoring information governance improvement plans.
- Reviewing and responding to information security incidents and breaches.
- Responding to wider information governance issues
- Maintaining productive relationships with external organisations such as the Information Commissioner, other public authorities and partner agencies.

1.5 In July 2015, the Information Commissioner's Office (ICO) was invited to conduct a consensual audit. The auditors visited KCC in October last year and issued their final report in January 2016. The executive summary was published on their website on 12th February.

https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/kent-county-council/

2. OUTCOME OF ICO AUDIT

2.1 The purpose of the audit was to provide the Information Commissioner and KCC with an independent assurance of the extent to which KCC, within the scope of this agreed audit, is complying with the DPA.

2.2 Recommendations were made in the three areas which were within the scope of the audit – 13 in relation to Training and Awareness, 26 with regard to Records Management and 15 concerning Data Sharing.

2.3 The ICO auditors felt that Training and Awareness was an area of limited assurance and therefore this report focusses primarily on this aspect of the audit.

2.4 The audit recognised the following **areas of good practice**:

- There is an Information Governance Communication Plan (IG Plan), which is produced each year. This sets out different ways of raising staff awareness around information governance.
- It was encouraging to hear that all staff within the Swale office Integrated Family Services had completed the records management e-learning training as mandatory induction training, despite not being mandatory for all staff corporately.
- KCC has a suite of policies, procedures and guidance to assist staff with data sharing. Topics covered include the responsibilities of Information Sharing Designated Officers (ISDOs), consent to share personal data, methods of transmitting personal data securely, and advice for handling requests for personal data. These policies and procedures are available on the staff intranet.
- KCC uses the ICO’s ‘Conducting Privacy Impact Assessments Code of Practice’ as a basis for its privacy impact assessments.

2.5 **Areas for improvement**

The auditors highlighted the following as areas where further action was required:

- There is no formal process to follow-up non-completion of data protection related training within services. The most recent IG e-learning completion statistics provided for the purposes of the audit showed that only 65% of staff had completed this mandatory training.
- Data protection related training needs have not been regularly assessed for all staff groups with access to personal data or for those with specific data handling and security management responsibilities.
- Records management performance measures have not been formally identified.
- KCC was not confident that all routine data sharing was supported by an Information Sharing Agreement, or an equivalent ‘Standard Operating Procedure’ (SOP), which removes an important layer of assurance that the data sharing is being managed properly. At the time of the audit, KCC was consulting on improvements to its data sharing

SOP and a draft copy of its proposed replacement SOP was provided for review.

2.6 The audit outcomes were reported to Corporate Directors in January and the response to the recommendations, all of which were accepted by that group, were agreed.

2.7 On 16 May, an update on progress made against the recommendations was reported to CMT.

2.8 The ICO will undertake a desk-based follow-up of the audit in July 2016. This will assess progress against recommendations demonstrated by KCC's completion of the Action Plan.

3. MANDATORY TRAINING PROGRAMMES RELATED TO INFORMATION GOVERNANCE AND DATA PROTECTION

3.1 **Induction**. All new entrants to KCC are required to complete an induction programme through e-learning. One of the sections of the programme is entitled "Protecting the people of Kent and KCC" and includes a module on information governance. The module explains that in order to comply with recommendations made by the Information Commissioner (ICO) and KCC's auditors, as well as best practice, all staff including temporary staff and contractors must complete the **Introduction to Information Governance** e-learning module. Staff need to have completed this and the Data Protection module within the first 3 months of working for KCC.

3.2 **Information governance e-learning.** This mandatory module is available to all staff and takes about 60 minutes to complete. The module outlines the importance of protecting information and runs through the measures staff should take both inside and outside of the workplace. There is also a section on sharing and sending information and a rundown of the roles and responsibilities of staff in the management of information, making this module a one-stop shop for all they need to know on information governance.

3.3 **Data protection e-learning.** This mandatory module is available to all staff and takes about 35 minutes to complete. The module aims to achieve a better understanding of staff's rights and responsibilities in protecting the rights of others. It will help people learn the meanings of terms used within the Data Protection Act and offers knowledge of the 8 principles of the Act and what they mean in practice.

4. ACTIONS AGREED FOLLOWING ICO AUDIT AND PROGRESS TO DATE

4.1 **Monitoring training uptake**. The statistics on take up of all mandatory training is provided monthly. The details, including the names of individuals yet to complete training, are provided to service Directors by the Business Partners with responsibility for HR. Mandatory training uptake is now also a regular agenda item on the Cross Directorate Information Governance Group.

4.2 The figures by Directorate for take up of the three relevant mandatory training programmes as at 30 April 2016 are shown at Appendix 2.

4.3 Whilst completion of the e-learning modules is mandatory for all staff, the emphasis for ensuring compliance has been on groups of staff who regularly access and handle sensitive data as part of their job. This emphasis is apparent from the differing take up rates across Directorates, with Social Care Health and Wellbeing and Strategic and Corporate Services (including HR and Finance activity) having higher take up than other areas.

4.4 It should also be noted that with the churn of staff, an organisation of this size will never achieve 100% take up of the training at any one time.

4.5 As well as the communication and engagement activity outlined in section 5 of this report, there are a number of actions being taken within individual Directorates to ensure that staff complete mandatory training. These include discussions at Directorate Management Teams and manager forums and at Directorate Organisation Development Groups.

4.6 Training is also available to Members through the Member induction e-learning module. At the time of writing this report, although six Members had started the module, none of the 84 members had completed it.

4.7 In reviewing completion of mandatory training it became apparent that not all those who had received training had had it recorded. This was for two main reasons. The first is that a small number of staff receive the training in face to face sessions as they do not have access to the on line option. It was clear that more communication was required about how to ensure these sessions were recorded on the individuals' learning records on the Oracle HR system. The second cause of under-reporting was that some staff were not going through the final stage of the e-learning process and evaluating the module, meaning that their completion was not recorded. Both these issues are being tackled by simplifying processes and improving communication.

4.8 **Changes to appraisal paperwork and process.** The ICO determined that training needs for all staff, including temporary and contract staff should be regularly assessed. In response to this and the need to maximize the uptake of compulsory training, the guidance for managers and paperwork associated with the appraisal process has been updated. The annual appraisal personal development plan form now has a space for managers and the appraisees to record the mandatory training that they have to complete and the guidance to managers reminds them that "You should include within Action Plans the requirement to undertake any appropriate mandatory training along with workforce planning for your teams".

5. ENGAGEMENT AND COMMUNICATION

5.1 Completion of mandatory training is an important aspect of managing risk around data breaches and safeguarding information, but awareness of the importance of information governance and data protection needs to be highlighted on an on-going basis to ensure everyone handling data on behalf of KCC is aware of their obligations and responsibilities.

5.2 An internal communications campaign has been put together for the period from May 2016 to February 2017, and is shown at Appendix 3.

5.3 The example below shows the article that appeared on the front page of KNet as part of the campaign.

Did you know?

We had 148 data security breaches last year! The main breaches were disclosing information to a third party in error and sending information to the wrong postal and email addresses. Make sure you understand the importance of protecting personal data and are familiar with our security policies. Find out the basic dos and don'ts. Make sure you've completed your mandatory training.

6. RECOMMENDATION

6.1 Policy and Resources Committee is asked to note and endorse the approach to information governance and data protection training outlined in this paper following the ICO audit.

Report Author:

Amanda Beer – Corporate Director Engagement, Organisation Design and Development , Strategic and Corporate Services, amanda.beer@kent.gov.uk