Report author: Carol Dunn
Tel: 0113 378 4574

**Report of: Chief Information Officer**

**Report to: Member Management Committee**

**Date: 23rd February 2016**

**Subject: Information Governance Training**

| | | |
|---|---|---|
| Are specific electoral Wards affected?<br>If relevant, name(s) of Ward(s): | ☐ Yes | ☒ No |
| Are there implications for equality and diversity and cohesion and integration? | ☐ Yes | ☒ No |
| Is the decision eligible for Call-In? | ☐ Yes | ☒ No |
| Does the report contain confidential or exempt information?<br>If relevant, Access to Information Procedure Rule number:<br>Appendix number: | ☐ Yes | ☒ No |

## Summary of main issues

1. The Data protection Act sets out individuals' and organisations' legal responsibilities with regard to people's personal data. These responsibilities are enforced by the Information Commissioners' Office (ICO) who have the power to impose monetary penalties of up to £500,000 for serious information security breaches.
2. Elected Members deal on a daily basis with personal data and sensitive personal data.
3. This report recommends providing Elected Members with suitable training and development to mitigate against and reduce the risk of Member involvement in an information incident.

## Recommendations

Member Management Committee is asked to note the contents of the report and support and approve the proposals to train Members on information governance as outlined in this report.

## 1 Purpose of this report

1.1 To seek support for a programme to deliver essential training and development for Members on Information Governance, with particular emphasis on handling personal data and compliance to the Data Protection Act.

## 2 Background information

2.1 The Data Protection Act controls how personal information is processed and stored by organisations. Everyone responsible for handling personal information has to follow rules known as the Data Protection Principles and ensure that information is processed and used fairly and lawfully.

2.2 The Information Commissioner's Office (ICO) is an executive non-departmental public body, sponsored by the Department for Culture, Media and Sport. The ICO upholds information rights in the public interest, promotes openness by public bodies and data privacy for individuals. The ICO has powers to take action to change the behaviour of organisations and individuals that collect, use and keep personal information, including criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice on a data controller.

2.3 In order to reduce the likelihood of enforcement action, the ICO recommends that data controllers deliver regular training about handling and processing personal data and the data protection principles within its organisation. To this end, all council staff undertake mandatory training on information governance and data protection every two years. In addition, staff who work with highly sensitive information receive additional classroom based training. This is important in order to ensure that all staff are aware of their responsibilities in respect of information governance and can take steps to avoid information security breaches. Furthermore, the council has provided an assurance to the ICO that staff will undertake regular IG training following a data protection audit conducted in 2013 by the Information Commissioner's auditors. .

2.4 Due to the nature of the work they do Members have access to and process personal and sensitive personal information which must be processed in accordance to the Data Protection Act. Members have more than one role; local councillors for a particular ward; membership of a political party; and members of various council committees, boards and groups, all of which will have them processing personal information in a different capacity.

2.5 The risks around information governance are often heightened for an Elected Member as a result of their public profile, media interest in their work and the sheer volume of correspondence exchanged with residents and organisations locally, regionally and nationally.

2.6 All LCC Members are annually registered with the ICO by the council as the Data Protection Act requires every data controller who is processing

personal data to register notification of this with the ICO. Members are considered to be data controllers in their own right when processing personal data on ward constituency matters.

## 3 Main issues

3.1 There have been many high profile information incidents reported by the media whereby the ICO has implemented enforcement action on organisations as a result of a security breach involving personal information, and the ICO has the power to issue a monetary penalty notice of up to £500,000. There are a number other tools available to the ICO for taking action to change the behaviour of organisations and individuals that collect, use and keep personal data, including prosecution of those who commit a criminal offence under the Act, issue of undertakings committing an organisation to a particular course of action in order to improve compliance and audit.

3.2 Furthermore the Data Protection Act allows an individual to ask for any information held about them, or in which they are mentioned, including information contained in emails. In addition the Freedom of Information Act gives individuals and organisations the right to ask for information held by a public body, and while there are certain exemptions that can be used, by and large those public bodies are obliged by an Act of Parliament to disclose that information. For example, it was as a result of an FOI request that information about MPs' expenses was released in 2009.

3.3 Member Management Committee considered a report about Information Governance Training at its meeting on 9th June 2012. Following consideration of this report, three Information Governance workshops were organised, at which a total of 19 members attended. High level training on Information Governance is delivered annually as part of the new Member induction programme. This training has been supported with communications to Members relating to specific information governance matters, such as information security issues related to email communications.

3.4 Most Members, if not all, now use technologies to process and store information. Because of the nature of their work, much of this information will be either personal or sensitive personal data. It is important that all Members handle and process personal information in accordance with the Data Protection Act and understand basic information governance practice around information security and information sharing. As a result of a request for IG training from Members with Adult Social Care responsibilities it is proposed that an information governance training and awareness programme for Member development is set up on the following basis:

- All LCC Members undertake basic IG training utilising an e-learning training package. This can be undertaken individually and at a time to suit individual Members. This training will provide Members with an elementary understanding of the Data Protection Principles and information security.

- In addition the Corporate Information Governance Team offer classroom-based sessions in order to address issues more specific to Members, especially in relation to the handling of sensitive personal data.

- Newly Elected Members continue to receive training on information governance as part of their induction programme.

## 4 Corporate Considerations

### 4.1 Consultation and Engagement

4.1.2 This report continues the process of engaging with Members about the most appropriate way of providing training and development to Members about information governance. Consultation has taken place with the Director of Adult Social Care, the Head of IM&T in Adult Social Care, Legal Services and with the council's Senior Information Risk Owner through the Information Management Board.

### 4.2 Equality and Diversity / Cohesion and Integration

4.2.1 All policies have been developed as part of the Information Governance Project which has developed a training programme for all staff and partners with respect to information governance. Equality, diversity, cohesion and integration are all being considered as part of this programme of work. This refers to the way in which the training is being delivered as well as how the policies will impact on staff and partners.

### 4.3 Council policies and City Priorities

4.3.1 The recommendations put forward in this report relate to ensuring that everyone within and associated with the council who handles and processes council information has an understanding of information governance policies.

4.3.2 The information governance policies relate to the aims, priorities and performance measures of the Council Business Plan and City Priority Plans.

### 4.4 Resources and value for money

4.4.1 Resources are already in place for the delivery of information governance e-learning for all staff. There are no financial or budgetary considerations with regard to classroom based training as this would be delivered in-house by members of the Corporate Information Governance Team.

### 4.5 Legal Implications, Access to Information and Call In

4.5.1 Whilst there is no legal requirement to ensure Members understand and comply with the council's information governance policies, there may be implications for the council if they inadvertently cause an information security breach to the Data Protection Act, and it follows therefore, that Members should obtain the same training, guidance and advice in this respect as officers.

4.5.2 There are no restrictions on access to information contained in this report.

## 4.6 Risk Management

4.6.1 The proposed training for Members is about not only making them aware of key aspects of council information governance policies and good information handling practice, but helping to reduce the risk of them inadvertently contributing to a potential information security incident.

## 5 Conclusions

5.1 This report provides Member Management Committee with information concerning the potential risks (both financial and reputational) around the handling of personal information, and recommends providing them with suitable training and development to mitigate against and reduce the risk of Member involvement in an information incident.

## 6 Recommendations

6.1 Member Management Committee is asked to note the contents of the report and support and approve the proposals to train Members on information governance as outlined in this report.

## 7 Background documents[1]

[1] The background documents listed in this section are available for inspection on request for a period of four years following the date of the relevant meeting. Accordingly this list does not include documents containing exempt or confidential information, or any published works. Requests to inspect any background documents should be submitted to the report author.