AGENDA ITEM
4

DATA PROTECTION

FALKIRK COUNCIL

Subject: **DATA PROTECTION**
Meeting: **EXECUTIVE**
Date: **7 June 2016**
Author: **DIRECTOR OF CORPORATE AND HOUSING SERVICES**

1. INTRODUCTION

1.1 Members may be aware of a data breach by the Council in March 2015, and the subsequent investigation by the Information Commissioner's Office (the ICO) into that incident. The Council's Chief Executive gave an undertaking to the ICO in November 2015 to improve on certain of the Council's practices in relation to data protection.

1.2 The purpose of this report is to provide Members with an update on work carried out in response to the undertaking and to seek approval of a new Data Protection Policy, as required by the undertaking.

2. BACKGROUND – ICO UNDERTAKING

2.1 The Council is a data controller as defined by the Data Protection Act 1998 (the Act). It has a duty to comply with the data protection principles set out in the Act in relation to all personal data in respect of which it is a data controller.

2.2 The data breach, which led to the undertaking, occurred following a subject access request (a request for information under the Act by an individual). The individual received the expected documents from the Council, with further documents relating to an unrelated third party.

2.3 The Council self-reported the breach to the ICO, which then investigated the incident and looked for the Council to enter into an undertaking to take certain actions to comply with the seventh data protection principle. The principle is that:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

3. SUMMARY OF PROGRESS

3.1 The table overleaf reports on progress against each of the 4 parts of the undertaking:

	Undertaking	Action
1	Within nine months, training will be provided to all staff members who handle personal data as part of their job role. This training will be mandatory and will be refreshed annually.	A short life working group has been established with representation from each Service to ensure that all staff who handle personal data are identified. Those with access to a Council computer are to complete an online training module. Those without access to a computer are to receive other forms of training. In both cases, training must be provided between 1 December 2015 and 31 August 2016 ie within the 9 month period stipulated by the undertaking. Thereafter, training will be repeated annually.
2	Within six months, a process for monitoring attendance at such training, or completion of online training, will be implemented, including steps to be taken when staff members have not attended/completed training. Corporate training KPIs will be reported to and over seen by a relevant senior management group or board.	The working group has agreed on the format of statistics to be reported to the Corporate Management Team annually. Failure to complete training will be considered a failure to follow a reasonable management instruction, and therefore subject to disciplinary action in the unlikely event that is necessary.
3	Within six months, improved guidance will be issued to staff members who routinely handle subject access requests. This will include details of the requirements of the Data Protection Act 1998 and how third party data should be dealt with.	Updated guidance has been prepared, reviewed by the working group, and added to the Council's intranet. This will be rolled out to staff who routinely handle subject access requests via the FOI/DPA Liaison Officers Group. The guidance is based on the ICO's own detailed guidance on subject access requests.
4	Within six months, produce a high level Data Protection Policy, setting out the data controller's commitments to the protection of personal data and the general standards it will adhere to. This is to be communicated to all relevant staff members within one month of completion, should link to the aforementioned subject access guidance and should be referenced in the mandatory training.	A data protection policy has been drafted, and is presented to Members for approval with this report (see Appendix). Once approved, the policy will be communicated to all staff and referred to in the mandatory training and on the data protection pages on the Council's intranet.

4. DATA PROTECTION POLICY

4.1 The proposed new policy is attached as an appendix to this report. The policy will supplement the existing Information Security Policy and Data Protection Guidelines, both of which are now due for review. Putting a new high-level policy in place is an opportunity for the Council to renew its commitment to adhering to the data protection principles.

4.2 The policy sets out 8 high level commitments, and includes a glossary and a summary of the data protection principles. Each of the 8 commitments will require further work to ensure compliance across the Council, including review of existing policies and procedures. This work will be taken forward by the Council's Information Governance Manager.

5. RECOMMENDATIONS

It is recommended that Members:

5.1 **approve the Data Protection Policy; and**

5.2 **note the steps taken by Officers to ensure compliance with the undertaking given to the ICO.**

..... ……..

DIRECTOR OF CORPORATE AND HOUSING SERVICES

Date: 25 May 2016

Ref: AAB070616 – Data Protection - WMB/LA/DP/31

Contact Officer: Wendy Barber, ext: 6043

APPENDIX

DATA PROTECTION POLICY

We process personal data in order to carry out our statutory functions. We are registered with the Information Commissioner's Office (ICO) as a data controller.

We are committed to protecting personal data and complying with the Data Protection Act 1998 (the Act) and the 8 data protection principles.

In terms of our Financial Regulations, the Director of Corporate and Housing Services, in consultation with the Chief Governance Officer, is responsible for ensuring that the requirements of the Act are complied with. Each Service Director is responsible for compliance with the Act by employees within their Service.

Our 8 core commitments

1. We will ensure that proper policies and procedures are in place to ensure compliance with the Act, in particular in the areas of Information Security and Records Management.
2. We will ensure that all staff who handle personal data understand their responsibilities under the Act and receive appropriate training annually.
3. We will ensure that our information technology systems protect the availability, integrity and confidentiality of personal data.
4. We will ensure that we tell data subjects what we will do with their personal data, by the use of fair processing notices.
5. We will ensure that procedures are in place to deal with subject access requests in line with the Act, and that we uphold other rights of data subjects under the Act.
6. We will ensure that we only share personal data with other organisations when appropriate and that it is shared safely and securely. Information sharing agreements will be put in place where regular sharing takes place.
7. We will ensure that we include appropriate clauses in contracts with third parties where they process personal data on our behalf.
8. We will ensure that any data breaches are handled in line with the ICO's guidance on data security breach management. All breaches will be recorded in a central log maintained by the Chief Governance Officer. Any serious breaches will be reported to the ICO.

Compliance with this policy, and related policies and procedures, is a condition of employment.

This policy will be reviewed every 3 years.

Summary of data protection principles

1. Personal data must be processed fairly and lawfully.
2. Personal data must be processed for limited purposes.
3. Personal data must be adequate, relevant and not excessive.
4. Personal data must be accurate and up-to-date.
5. Personal data must not be kept for longer than is necessary.
6. Personal data must be processed in line with the data subject's rights.
7. Personal data must be secure.
8. Personal data must not be transferred to other countries without adequate protection.

Glossary

Data
Recorded information of any kind, including information held in a form which can be processed by computer.

Personal data
Data which relates to a living individual who can be identified (a) from that data or (b) from that data and other information in the possession of the data controller. This includes an expression of opinion about the individual.

Data controller
A person who determines the purpose for which, and the manner in which, any personal data are, or are to be, processed.

Processing
Includes obtaining, recording, holding, using, adapting, altering, disclosing, deleting or erasing.

Data subject
An individual who is the subject of personal data.

Subject access request
A written request by an individual to a data controller under section 7 of the Act, usually for any personal data processed by the data controller of which s/he is the data subject.