ABERDEEN CITY COUNCIL

COMMITTEE	AUDIT & RISK COMMITTEE
DATE	20TH NOVEMBER 2014
DIRECTOR	EWAN SUTHERLAND
TITLE OF REPORT	DATA PROTECTION REPORTING – JULY – SEPTEMBER 2014
REPORT NUMBER:	CG/14/139
CHECKLIST RECEIVED	YES

1. PURPOSE OF REPORT

The purpose of this report is to provide an overview for quarter 2 (July – September 2014) to Committee of the following areas:

a) Aberdeen City Council Subject Access Request statistics
b) Data Breaches and Near Misses
c) Data Protection training
d) General Update

2. RECOMMENDATION(S)

It is recommended that the Committee note the report.

3. FINANCIAL IMPLICATIONS

There are no financial implications at this time.

4. OTHER IMPLICATIONS

None

5. BACKGROUND/MAIN ISSUES

a) Aberdeen City Council Subject Access Request Statistics

A recommendation of the Information Commissioners Office (ICO) inspection of the Council's compliance with Data Protection legislation

was that the number of Subject Access Requests (SARs) and Third Party Requests received by the Council be recorded and reported to the appropriate Committee. As previously advised, these figures will be reported to the Audit & Risk Committee on a quarterly basis. The figures for the latest complete quarter, July – September 2014, are detailed below. As this quarter relates to the Council structure prior to the 5th October 2014 restructure, these are detailed in the former service names. The next quarterly report will reflect the revised structure arrangements.

In the reporting quarter Aberdeen City Council received **33** Subject Access Requests and **48** requests from 3rd parties for personal data held by it.

By Service:

Service	Subject Access Requests	3rd Party Requests
Office of Chief Executive	**0**	**0**
Corporate Governance	**1**	**0**
Education, Culture & Sport	**2**	**0**
Enterprise, Planning & Infrastructure	**0**	**2**
Housing & Environment	**5**	**9**
Social Care & Well Being	**25**	**37**
TOTAL	**33**	**48**

The requirement of the Data Protection Act is that requests are responded to within 40 days. **67** requests were responded to within 40 days in the reporting quarter, some **82.72%** of requests received.

The Council can charge a fee, maximum of £10, prior to responding to a Subject Access Request. In the reporting period fees were charged in respect of **3** requests.

b) <u>Data Breaches</u>

In addition to the above, the Council has an established procedure for the recording and reporting of data protection breaches. This information is reported to Members in order to provide an overview of the Council's performance in relation to keeping personal data secure.

In the reporting quarter the following breaches occurred:

By Service:

Service	Number of Breaches
Office of Chief Executive	0
Corporate Governance	3
Education, Culture & Sport	0
Enterprise, Planning & Infrastructure	1
Housing & Environment	0
Social Care & Well Being	2
TOTAL	**6**

By Breach Type:

Type of Breach	Number of Breaches
Human Error	4
Unauthorised Disclosure	1
Unauthorised Access	0
Loss	0
Theft	1
Other	0
TOTAL	**6**

Data Protection breaches are dealt with in a way which is dependent on the nature and potential severity of the breach. Where a breach involves or potentially involves a large volume of personal data or sensitive personal data which is likely to have an adverse impact of the data subject, then more often than not, the Council as Data Controller will 'self-report' the breach to the ICO.

During the reporting period none of the breaches were such that a self-report to the ICO was required. One incident was reported to the Police.

The regular reports to this Committee will also provide an opportunity to update Members in relation to any significant breaches, including those where the Council has 'self-reported'. It will also allow for an update in respect of previous significant breaches, particularly where there may have been media coverage.

There have been no determinations by the ICO of outstanding breach investigations during the reporting period.

The Council's Data Protection Breach Reporting Procedure is in the process of being reviewed by Officers in the Legal Services Commercial & Advice Team. The purpose of this review is to simplify reporting mechanisms and clarify when a report is required. It is hoped that this review will assist in ensuring a consistent and robust approach to the recording of data protection breaches.

c) Near Misses

As previously reported to Committee, the recording of breaches is to be enhanced by the incorporation of data protection near misses.

A data protection near miss is defined as 'a situation which did not result in a data protection breach occurring, but had the potential to do so'. It is envisaged that the reporting and monitoring of near misses will enable the identification of the causes of data protection risk situations and of procedural and / or training deficits which require to be addressed.

A draft Near Miss reporting framework will be incorporated into the reviewed Breach reporting procedure in due course.

d) Data Protection Training

The OIL Training Course 'Data Protection Principles' is a mandatory course which is to be completed by all employees. Despite this position, completion rates for this training are low (under 40%) and there is currently little or no monitoring by management of uptake.

Adherence to the requirement to complete this training is an important requirement as it enables the Council to demonstrate to the ICO that duties in respect of data protection are cascaded to all employees.

The Commercial and Advice Team is presently exploring options for supporting a more rigorous completion and monitoring framework for this mandatory training. These options will be reported to CMT in due course for consideration.

Additionally, feedback from the Organisational Development team indicated that the content of the training should be reviewed in order to ensure that key messages and expected behaviour were clearly stated.

As such, the content of the induction data protection training has been reviewed and is currently being redesigned. There will be core training which will require to be completed by all Council staff, with additional topics for staff working in Education services and staff working in Social Work services which will require to be completed. The training will be available via the on-line learning portal, OIL, and in paper format for staff without access to IT equipment. It is planned that the reformatted training will be launched in early 2015.

A further aspect of data protection training that is currently being developed is refresher training. It is envisaged that refresher training will be a requirement on all staff and for any person changing jobs. The Commercial & Advice Team are presently reviewing suitable periods for such refresher training to be required, based on the notional risks of different parts of the organisation. It is currently planned that refresher training will be available from Spring 2015.

6. IMPACT

None

7. MANAGEMENT OF RISK

Adherence to the Council's policies and procedures for the handling of personal data is essential to the management of the risk associated with the management of information. Strong monitoring of the effectiveness of these arrangements is necessary in order to identify any areas of concern and implement appropriate arrangements to mitigate this.

8. BACKGROUND PAPERS

None

9. REPORT AUTHOR DETAILS

Fiona Smith, Governance Support Officer

E-mail: fismith@aberdeencity.gov.uk
Telephone: 01224 522516