

ABERDEEN CITY COUNCIL

COMMITTEE	AUDIT & RISK COMMITTEE
DATE	26 TH FEBRUARY 2015
DIRECTOR	EWAN SUTHERLAND
TITLE OF REPORT	DATA PROTECTION REPORTING – OCTOBER – DECEMBER 2014
REPORT NUMBER:	CG/15/21
CHECKLIST RECEIVED	YES

1. PURPOSE OF REPORT

The purpose of this report is to provide an overview for quarter 3 (October - December 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, October - December 2014, are detailed below.

In the reporting quarter Aberdeen City Council received **17** Subject Access Requests and **35** requests from 3rd parties for personal data held by it.

By Service:

Service	Subject Access Requests	3 rd Party Requests
Office of Chief Executive	0	0
Communities, Housing & Infrastructure	8	5
Corporate Governance	1	0
Education & Children's Services	8	30
TOTAL	17	35

In the quarter, **40** requests have been responded to. The requirement of the Data Protection Act is that requests are responded to within 40 days. **38** requests were responded to within 40 days in the reporting quarter, some **95%** of requests responded to.

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 **14** requests.

b) Data Breaches and Near Misses

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

Communities, Housing & Infrastructure	2
Corporate Governance	0
Education & Children's Services	3
TOTAL	5

By Breach Type:

Type of Breach	Number of Breaches
Human Error	4
Unauthorised Disclosure	0
Unauthorised Access	1
Loss	0
Theft	0
Other	0
TOTAL	5

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.

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.

As reported previously, a review of the Council's Data Protection Breach Reporting Procedure is underway. The review is meantime being conducted by officers in the Commercial & Advice Team of Legal

Services and, in due course, will engage with Operational Support colleagues across the Council to ensure the views and experiences of services underpin the new policy and procedure. It is planned that this review will be completed by the end of March 2015 and that the revised policy and procedure will be submitted to CMT in April 2015 and then to Audit, Risk & Scrutiny Committee in June 2015.

The purpose of this review is to simplify reporting mechanisms, to clarify when a report is required and to introduce arrangements for the recording and reporting of near misses. It is hoped that this review will assist in ensuring a consistent and robust approach to the recording of data protection breaches and will also encourage the reporting of near misses as a matter of course, in order that the Council can learn from these and amend policy and practice as required.

c) Data Protection Training

As previously reported to Committee, a review of induction Data Protection is underway. This induction training is mandatory for all staff and the purpose of the review is to ensure that the contents and delivery of the training meet the requirements of the Council, Services and individual staff and take cognisance of assessed risk areas. Additionally, options for refresher training will also be built into the available training package.

Officers undertaking the review have engaged with officers in the Organisational Development team in order to ensure that the revised training meets recognised standards for training and that the training is delivered in a range of formats in order to be accessible to all employees.

It is envisaged that this review will be completed by the end of April 2015, testing of revised training commencing shortly thereafter with roll out, subject to approval, starting in June 2015.

As completing the Induction Training is a mandatory requirement for all staff, consideration is also being given to options for monitoring and ensuring compliance. It is planned that a report on options for this will be taken to CMT in April 2015 and further reported to Audit, Risk & Scrutiny Committee in June 2015.

d) Complaints about Data Handling

A further aspect of the Data Protection responsibilities of Aberdeen City Council is responding to any complaints received from data subjects relating to the manner in which the Council processes their personal data.

The process for handling complaints is two-fold. At the first stage, when the complaint is raised with the Council, the organisation will

seek to respond to the complainant and resolve the concern. This may be by providing information relating to the manner in which personal data has been processed or by identifying and rectifying any weakness.

The second stage, if a complainant remains dissatisfied is where a data subject can make a complaint to the ICO. The ICO will invite the Council to advise of its handling of the issue under consideration and thereafter investigate such complaints and determine whether or not it is likely that the Council has fulfilled its obligations and duties under the Data Protection Act.

If the Council has failed in its obligations and duties, the ICO can require the organisation to take action to mitigate any risk.

In the reporting period, **1** complaint was received by the Data Controller from a data subject.

Further, in the reporting period, the ICO notified the Council that **1** complaint had been received in its office. The Council responded to the complaint and the ICO's determination is awaited.

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