ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk & Scrutiny
DATE	27 June 2016
INTERIM DIRECTOR	Richard Ellis
TITLE OF REPORT	Data Protection Reporting (Annual Report: April 2015 - March 2016)
REPORT NUMBER:	CG/16/089
CHECKLIST RECEIVED	Yes

1. PURPOSE OF REPORT

To provide an overview for the previous financial year (April 2015 - March 2016) in relation to Council data protection matters including Subject Access Requests, Third Party Requests, breaches, complaints and training.

This is the first such annual report. Future annual reports will contain comparisons with previous years and analysis of trends. Reference is also made to the "Data Protection Reporting (January - March 2016)" quarterly report which is also being considered at this Committee meeting and which contains comparisons between quarters.

2. RECOMMENDATION(S)

That the Committee note the report.

3. FINANCIAL IMPLICATIONS

None.

4. OTHER IMPLICATIONS

None.

5. BACKGROUND/MAIN ISSUES

Data protection is governed by the Data Protection Act 1998 (the Act) and the Information Commissioner's Office (ICO) enforces compliance. The Council is a Data Controller under the Act and, as such, has various responsibilities.

5.1 Subject Access Requests and Third Party Requests

A Subject Access Request (SAR) is a request made to an organisation by or on behalf of an individual for his/her own personal data held by the organisation. A Third Party Request (TPR) is a request made to an organisation by a third party (e.g. Police Scotland, HMRC, the Care Inspectorate, a local authority) for personal data about an individual held by the organisation.

Numbers of Requests

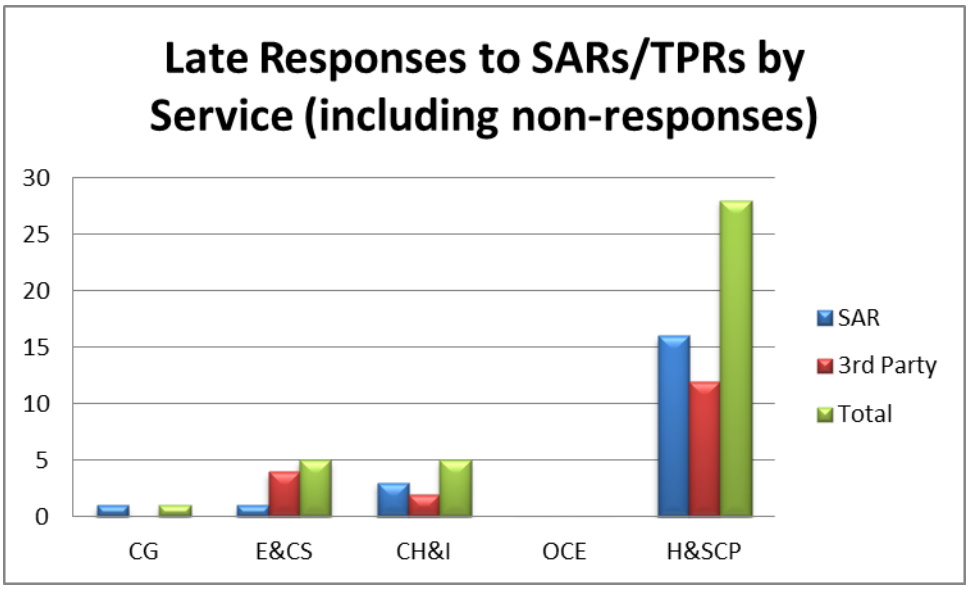
Statistics are reported to this Committee on a quarterly basis and the figures for the whole year (April 2015 - March 2016) are detailed below.

Directorate/Service	SARs	TPRs
Aberdeen City Health & Social Care Partnership	60	187
Communities, Housing & Infrastructure	10	78
Corporate Governance	7	0
Education & Children's Services	7	15
Office of the Chief Executive	0	0
Sub Total	**84**	**280**
Total Received	**364**	

Response Times/Late Responses

In this year, 325 of the 364 requests **(89%)** were responded to within 40 days. The Act requires SARs to be responded to within 40 days and the Council would normally expect to respond to TPRs within that timescale. The table and bar chart below show the numbers of responses (SARs and TPRs) that were outwith the 40 day timescale for each Directorate/Service in the reporting year.

Directorate/Service	SARs	TPRs	Total
Corporate Governance	1	0	1
Education & Children's Services	1	4	5
Communities, Housing & Infrastructure	3	2	5
Office of the Chief Executive	0	0	0
Aberdeen City Health & Social Care Partnership	16	12	28



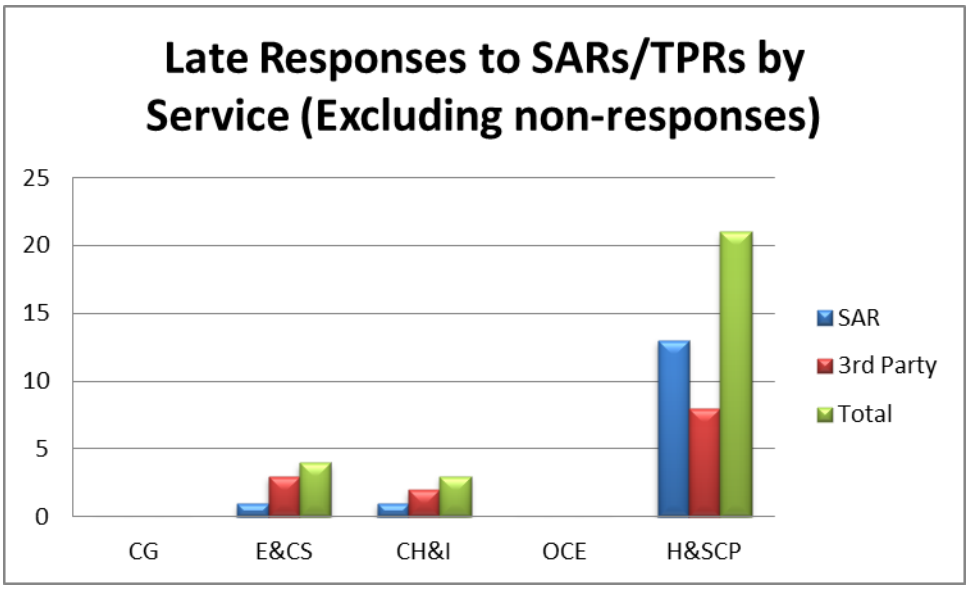
In this year, there were **39** late SAR or TPR responses.

The lateness of these responses was largely due to the extensive staff time and resource involved in examining multiple voluminous records to remove third party data and make appropriate redactions. Some requests in relation to social work records may require the careful review of thousands of pages.

The above figures include both late responses and non-responses. A non-response can be for various reasons, such as a requester not replying to a request for clarification or a request for payment.

When non-responses are excluded, the figures are as follows:

Directorate/Service	**SARs**	**TPRs**	**Total**
Corporate Governance	0	0	0
Education & Children's Services	1	3	4
Communities, Housing & Infrastructure	1	2	3
Office of the Chief Executive	0	0	0
Aberdeen City Health & Social Care Partnership	13	8	21



Charging Fees for SARs

The Council may charge a fee (maximum £10) prior to responding to a SAR. Each Directorate/Service determines whether it will charge a fee in an individual case. In this year, fees were charged in respect of **6** SARs.

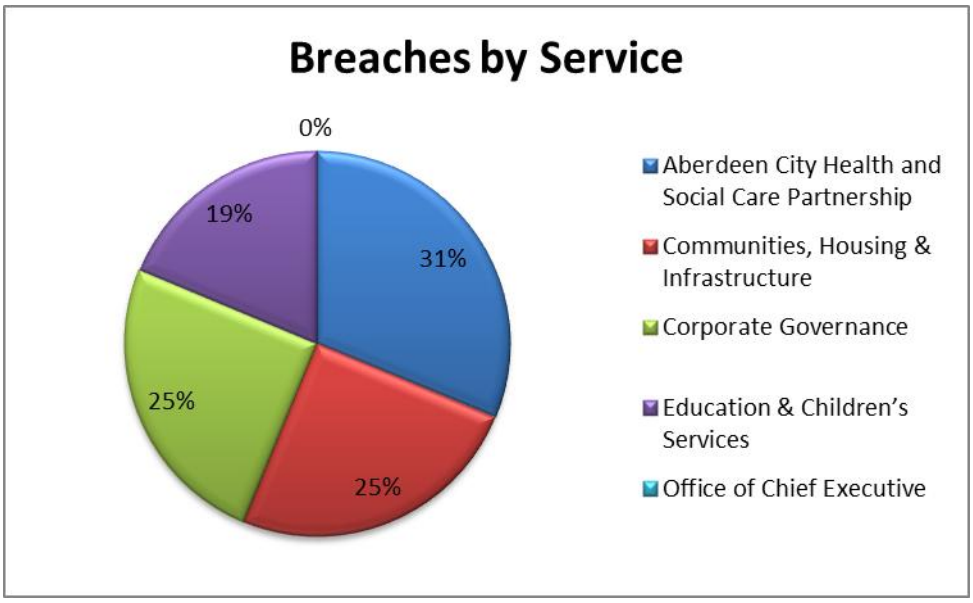
With regard to social work SARs, charges would generally only be imposed in the case of repeat requests and it is considered desirable that service users are generally able to freely access their information without barriers being placed in their way.

5.2 Data Protection Breaches

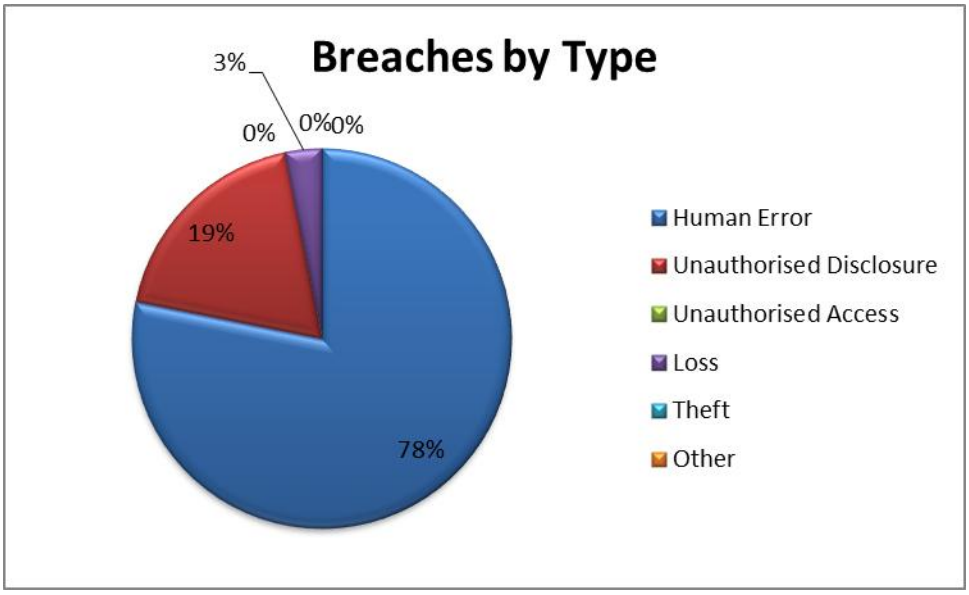
A data protection breach is basically a failure to comply with data protection law which results in loss, release or corruption of personal data. Examples are unauthorised access to, use of or disclosure of personal data and failure to destroy or retain such data appropriately.

In this year, the following breaches occurred (by Directorate/Service and breach type):

Directorate/Service	No. of Breaches
Aberdeen City Health & Social Care Partnership	10
Communities, Housing & Infrastructure	8
Corporate Governance	8
Education & Children's Services	6
Office of the Chief Executive	0
Total	**32**



Type of Breach	No. of Breaches
Human Error	25
Unauthorised Disclosure	6
Unauthorised Access	0
Loss	1
Theft	0
Other	0
Total	**32**



Data breaches are reported to the Head of Legal and Democratic Services. Legal Services liaise with the relevant Service in order to provide advice and determine what action requires to be taken. Breaches are dealt with according to their nature and seriousness, with careful regard being had to ICO guidance. Where there is significant actual or potential detriment - whether because of the volume of data, its sensitivity or a combination of the two - the Council as Data Controller will normally 'self-report' the breach to the ICO.

In this year, **2** self-reports were made to the ICO. One concerned the temporary loss of an encrypyted USB stick (it is vitally important that such devices are encrypted) which was recovered soon after and the other concerned the unauthorised disclosure, in error, of an individual's sensitive personal data to a family member.

There has been **1** determination by the ICO of outstanding breach investigations during this year. This related to the USB stick incident mentioned above. The ICO decided that no further action was necessary and closed the case. The ICO considered it unlikely that there had been a data protection breach because, at the time of the incident, the Council had appropriate organisational and technical measures in place to protect the data. This was back-up data (and not the only copy) and the Council had encryption, suitable policies, procedures and staff training in place. The ICO also noted that the two relative weaknesses in the process (returning the USB stick with data still on it and having to post and collect the device) were being addressed.

5.3 Complaints about Data Handling

If an individual is dissatisfied with the Council's response to his/her complaint about data handling, s/he may make a complaint to the ICO. The ICO will investigate and may take action against the Council.

In this year, **2** complaints were received by the Council and **1** notification was received from the ICO regarding a complaint against the Council. The notification received from the ICO concerned the sharing of personal data without written consent (the giving of verbal consent having been disputed).

5.4 Data Protection Training and other matters

The e-induction module was launched in late May 2016. Further consideration will be given to how completion rates for this training will be monitored.

A new Corporate Data Protection Policy was approved by the Finance, Policy and Resources Committee on 15 September 2015 and is available in the Data Protection section of The Zone.

6. IMPACT

Improving Customer Experience – it is in the interests of all the Council's customers and service users that the Council handles their personal data lawfully and that they are able to access it timeously on request.

Improving Staff Experience – the provision of appropriate training, as mentioned above, should ensure Council staff are confident and capable in undertaking their data protection responsibilities.

Improving our use of Resources – by reporting to Members on statistics and trends, this report should assist the Council in fulfilling its data protection responsibilities more efficiently.

Corporate – compliance by the Council with its data protection responsibilities is integral to individual Service Plans and the "Aberdeen – the Smarter City" vision.

Public – this report may be of interest to the public in that it concerns the Council's compliance with its data protection obligations. This report will not impact adversely on any particular group and so neither an Equality and Human Rights Impact Assessment (EHRIA) nor a Privacy Impact Assessment (PIA) is necessary.

7. MANAGEMENT OF RISK

Compliance with the Act and the Council's relevant policies and procedures is essential to the management of the risk associated with data handling. Strong monitoring of the Council's compliance should help identify risks and the actions required to mitigate those risks.

8. BACKGROUND PAPERS

None.

9. REPORT AUTHOR DETAILS

Steven Inglis, Team Leader, Governance Team, Legal Services

Email: singlis@aberdeencity.gov.uk

Telephone: 01224 523168