Local Government Information Governance Survey

The Information Commissioner's Office carried out this survey, about the governance of data protection and freedom of information, in 2016 to identify common areas of both good practice and possible improvement.

The survey was open to local councils, excluding parish and town councils.

Councils were advised to make one submission, ideally completed by their information governance lead.

ico.
Information Commissioner's Office

20 March 2017

Introduction

Where is your council based?

136 (78.6%) England

4 (2.3%) Northern Ireland

18 (10.4%) Scotland

15 (8.7%) Wales

How is your council structured?

105 (60.7%) Unitary

68 (39.3%) Two - tier

Management structures

Has your council established the following information governance roles?

	Yes	No
Senior Information Risk Owner (SIRO)	155 (89.6%)	18 (10.4%)
Data Protection Officer (DPO)	128 (74.0%)	45 (26.0%)
Information Governance Manager	113 (65.3%)	60 (34.7%)
Information Security Manager (responsible for the security of both manual and electronic personal data, and therefore distinct from an Information Technology (IT) Manager)	96 (55.5%)	77 (44.5%)
Records Manager	84 (48.6%)	89 (51.4%)
Information Asset Owners (IAOs)	114 (65.9%)	59 (34.1%)
Lead individual requests for information under the Data Protection Act 1998 and the Freedom of Information Act 2000 (dedicated post or forming part of other post such as DPO)	164 (94.8%)	9 (5.2%)

Are these information governance roles currently occupied?

	Yes	No
Senior Information Risk Owner (SIRO)	151 (97.4%)	4 (2.6%)
Data Protection Officer (DPO)	123 (96.1%)	5 (3.9%)
Information Governance Manager	112 (99.1%)	1 (0.9%)
Information Security Manager (responsible for the security of both manual and electronic personal data, and therefore distinct from an Information Technology (IT) Manager)	91 (94.8%)	5 (5.2%)
Records Manager	79 (94.0%)	5 (6.0%)
Information Asset Owners (IAOs)	109 (95.6%)	5 (4.4%)
Lead individual requests for information under the Data Protection Act 1998 and the Freedom of Information Act 2000 (dedicated post or forming part of other post such as DPO)	162 (98.8%)	2 (1.2%)

Has your council established a corporate information governance group?

120 (69.4%) Yes

53 (30.6%) No

Approximately how often does it meet?

5 (4.2%) Occasionally

60 (50.0%) Every 4-6 weeks

51 (42.5%) Every 3 months

4 (3.3%) Every 6 months

0 (0.0%) Annually

Are the following post holders members of the group?

	Yes	No
Senior Information Risk Owner (SIRO)	95 (79.2%)	25 (20.8%)
Information Governance Manager	87 (72.5%)	33 (27.5%)
Data Protection Officer (DPO)	79 (65.8%)	41 (34.2%)
Information Security Manager	67 (55.8%)	53 (44.2%)
Information Technology (IT) Manager	87 (72.5%)	33 (27.5%)
Records Manager	49 (40.8%)	71 (59.2%)
Caldicott Guardian	53 (44.2%)	67 (55.8%)
Information Asset Owners (IAOs)	53 (44.2%)	67 (55.8%)

Information Risk Management

Has your council established an Information Asset Register (IAR)?

101 (58.4%) Yes, partially completed

30 (17.3%) Yes, fully completed

42 (24.3%) No

Does your council have any risk registers?

165 (95.4%) Yes

8 (4.6%) No

Do any of the risk registers explicitly include information risk issues?

135 (81.8%) Yes

30 (18.2%) No

Does your council undertake Privacy Impact Assessments (PIAs) to identify and reduce the privacy risks of any new process or project?

114 (65.9%) Yes

59 (34.1%) No

Does your council have contracts in place with data processors which explicitly impose obligations equivalent to the seventh data protection principle (security) upon them?

90 (52.0%) Yes, with all of our data processors

72 (41.6%) Yes, but only with some of our data processors

11 (6.4%) No

Does your council maintain a corporate log / register of information security breaches?

153 (88.4%) Yes

20 (11.6%) No

Approximately how often do you review this to identify common causes?

32 (20.9%) Occasionally

54 (35.3%) Every 4-6 weeks

39 (25.5%) Every 3 months

8 (5.2%) Every 6 months

15 (9.8%) Annually

5 (3.3%) Never

Compliance and assurance

In order to monitor compliance, does your council regularly generate reports and establish Key Performance Indicators (KPIs) for each of the following?

	Reports	KPIs	Neither
Number and percentages of subject access and freedom of information requests complied with within statutory timescales	141 (81.5%)	83 (48.0%)	14 (8.1%)
Number and nature of information security breaches	133 (76.9%)	21 (12.1%)	38 (22.0%)
Number and percentage of the workforce who have completed mandatory data protection training	117 (67.6%)	44 (25.4%)	46 (26.6%)

Who has responsibility for checking the information generated in the reports against the KPIs?

67 (47.9%) Corporate information governance group

0 (0.0%) Management Team or Chief Executive and Corporate Directors

44 (31.4%) Heads of Service or equivalent

34 (24.3%) Audit / Scrutiny Committee or equivalent

29 (20.7%) No one

Does your council's annual audit programme explicitly incorporate data protection / information governance related issues?

53 (30.6%) Always

69 (39.9%) Regularly

41 (23.7%) Infrequently

10 (5.8%) Never

Does your council align to or comply with the following standards?

	Yes	No
Local Public Services Data Handling Guidelines 2014	84 (48.6%)	89 (51.4%)
NHS Information Governance Toolkit (social care)	77 (44.5%)	96 (55.5%)
ISO 27001	153 (88.4%)	20 (11.6%)
Payment Card Industry Data Security Standard (PCI DSS)	75 (43.4%)	98 (56.6%)
Government Security Classifications post 2 April 2014 (Official, Official - sensitive, Secret, Top Secret)	138 (79.8%)	35 (20.2%)

Policies

Does your council have the following policies in force?

	Yes	No
Information Governance Framework / Strategy	121 (69.9%)	52 (30.1%)
Data Protection Policy	161 (93.1%)	12 (6.9%)
Information Security Policy	162 (93.6%)	11 (6.4%)
Information Security Incident Management Policy (standalone policy or incorporated elsewhere)	149 (86.1%)	24 (13.9%)
Information Risk Policy	75 (43.4%)	98 (56.6%)
Privacy Impact Assessment (PIA) Policy	76 (43.9%)	97 (56.1%)
Records Management Policy	134 (77.5%)	39 (22.5%)
Subject Access Policy	125 (72.3%)	48 (27.7%)
Freedom of Information Policy	144 (83.2%)	29 (16.8%)
Data Sharing Policy	109 (63.0%)	64 (37.0%)

Approximately how often does your council review information governance policies?

26 (15.0%) Occasionally

75 (43.4%) Every year

44 (25.4%) Every two years

24 (13.9%) Every three years

4 (2.3%) Never

Training

Does your council have mandatory data protection training for all employees who process personal data?

142 (82.1%) Yes

31 (17.9%) No

Is completion of data protection training a precondition of network and / or systems access?

42 (29.6%) Yes, for some network and / or systems access

24 (16.9%) Yes, for all network and / or systems access

76 (53.5%) No

Does your council have mandatory data protection refresher training for all employees who process personal data?

100 (70.4%) Yes

42 (29.6%) No

Approximately how often do employees undertake refresher training?

6 (6.0%) Occasionally

59 (59.0%) Every year

26 (26.0%) Every two years

9 (9.0%) Every three years

Does your council provide or arrange specialised training for the following roles?

	Yes	No
Senior Information Risk Owner (SIRO)	91 (52.6%)	82 (47.4%)
Information Asset Owners (IAOs)	71 (41.0%)	102 (59.0%)
Information Governance Manager	77 (44.5%)	96 (55.5%)
Data Protection Officer	98 (56.6%)	75 (43.4%)
Information Security Manager	76 (43.9%)	97 (56.1%)
Information Technology (IT) Manager	92 (53.2%)	81 (46.8%)
Records Manager	55 (31.8%)	118 (68.2%)
Individuals responsible for processing freedom of information requests	124 (71.7%)	49 (28.3%)
Individuals responsible for processing subject access requests	129 (74.6%)	44 (25.4%)