CC50.9 - 2014

CYNGOR SIR *POWYS* COUNTY COUNCIL

County Council
30th April 2014

REPORT AUTHOR: **County Councillor Steve Davies, Portfolio Holder for HR ICT and Communications**

SUBJECT: **Question from County Councillor Kathryn Silk**

Could the Cabinet Member explain how many breaches of the Data Protection Act there were involving data held by Powys County Council over the last year for which figures are available; which service area was involved in the case of each breach; how many of these breaches related to sensitive personal information; if he is satisfied that measures taken to prevent breaches of the Act are adequate; and if he will provide three-monthly figures to councillors detailing any breaches that occur in future.

For the financial year 01-04-13 to 31-03-14 there were 99 reported Information Security Incidents.

Of those 99, following investigation, 55 were established as having breached the Data Protection Act 1998.

Service Area	**Numbers of breaches**
Housing	4
Business Support	11
Provider of Services	4
Children's Services	11
Legal Services	1
Development Management	2
Schools Services	3
IT	1
Adult Services	5
Income & Awards	3
Customer Services	2
Youth Services	1
HR	3
Information Management Unit	3
CYPP	1
Total	**55**

- 29 of these 55 breaches occurred internally within the Council, with 26 having occurred externally to the Council

- 21 of these 55 breaches involved sensitive personal data (as defined under the Act)

- 40 of these 55 breaches were contained, i.e. recipients confirm deletion, destruction or returned personal data.

Every local authority is responsible for the processing of vast amounts of personal information in respect of customers, residents, service users, and staff; this information is accessed by and used by thousands of staff in the process of their daily work. There will be times when simple errors cause data protection breaches to occur.

It is a requirement of the Data Protection Act 1998 that these local authorities ensure that where ever possible measures are in place to protect the personal information being used, with the cost of those measures being appropriate to the nature of the personal information being protected and the likely harm that would result should an information security incident occur.

One measure employed by Powys County Council is the training of all staff with access to personal data, in the basics of the Data Protection Act 1998, and the organisation's policies and procedures in relation to information handling.

Current training figures stand at 99%.

The development of training processes and the monitoring of compliance has been undertaken by the Corporate Information Governance Group, in addition to its overseeing of practices developed to manage information risks.

Some of these centrally recorded information security incidents do not qualify as a breach of the Data Protection Act 1998 but they do inform Powys County Council of areas of weakness or risk to be acted upon.

Others are considered information breaches under the particulars of the Data Protection Act 1998, but are contained within the organisation, and are not within the public domain.

The Information Commissioner's Office has previously advised Powys County Council, that they are satisfied that either the Council has or intends to implement appropriate policies and procedures suitable to prevent re occurrences of information security incidents, similar to those previously brought to their attention.

Powys County Council was subject to a consensual audit last year, undertaken by the Information Commissioner's Office, to consider its compliance with the Data Protection Act 1998. The Council's assurance level was determined as ***reasonable***, indicating that the auditors felt there is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance, for the scope areas examined.

The ICO utilises four assurances ratings which are graded from very limited, limited, reasonable, and high.

The outcome of the audit has informed the future work programme of both the Corporate Information Governance Group and Corporate Information Operational Governance Group.

Thus based on those practices put in place and those which continue to be developed it can considered that the Council is actively developing systems to safeguard compliance with information legislation, including the reporting and management of Information Security Incidents.

Since Information Security Incidents are reported and recorded centrally, figures can be supplied quarterly, to the portfolio holder, by the Corporate Information Governance Group.