ISLE OF ANGLESEY COUNTY COUNCIL	
Report to	**Audit and Governance Committee**
Date	**15 March 2016 @ 2pm**
Subject	**Information Governance – ICO's Enforcement Notice**
Lead Officer	**Lynn Ball, Head of Function (Council Business)/Monitoring Officer**
Contact Officer	**Lynn Ball, Head of Function (Council Business)/Monitoring Officer** **lbxcs@anglesey.gov.uk** **01248 752586**
Nature and reason for reporting – At the request of the Committee	

Introduction

Public authorities hold a significant amount of information about individuals. How we use that information, and our obligations to keep that information safe, creates risks. The main statutory driver is the Data Protection Act 1998, and a significant breach, or repeated lower level breaches, may result in a significant monetary penalty, up to a maximum of £500k. Additionally, if data about individuals is wrongly shared or disclosed, thereby causing them harm, they are entitled to compensation; with the potential for substantial awards depending on the level of harm and distress caused.

Since 2013, the Council has invested significantly in improving its compliance with the Data Protection Act and has in place the relevant policies and procedures to support compliance with the Act by managing the risks inherent in creating, storing and using information about living individuals. Arrangements are in place to ensure that all staff are trained appropriately and that compliance is monitored; although these two areas require further embedding.

Background

The Council was required to sign formal Undertakings with the Information Commissioner, the UK regulator for the Data Protection Act, in January 2011 and December 2012. Following a significant number of data security incidents, within a short timeframe, the Information Commissioner's Office (ICO), in 2012, undertook a consensual audit of the Council's arrangements for data protection. The ICO issued its report in 2013 which contained a number of recommendations. The Council established a Corporate Information Governance Project Board to formulate and deliver an Action Plan to implement the required improvements. This was agreed with the ICO.

Almost a 100 agreed objectives had been fully realised by the time of the re-audit by the ICO in 2014. The re-audit recognised improvements on the earlier findings but an additional 66 activities were required by the ICO, the vast majority of which constituted additional recommendations over and above those achieved following the original audit in 2013.

The Project having concluded, in November 2014 the Council established a Corporate Information Governance Board (CIGB), chaired by the Senior Information Risk Owner (SIRO), as a vehicle for delivering the new Action Plan arising from the re-audit. These included short and medium term objectives followed by ongoing oversight and responsibility for data protection compliance.

Despite evidence of clear progress in achieving the new objectives, the Council was still issued with an Enforcement Notice by the ICO in October 2015. This occurred even though the Council had been able to provide significant evidence to demonstrate that it had deployed time and resources into implementing the changes required by the ICO, as identified in both audits.

The issues highlighted in the Enforcement Notice's nine recommendations are now the subject of a third Action Plan, devised by the CIGB, and being implemented by a sub-group of the CIGB. Work and resources have had to be reprioritised to ensure that the activities that would best defend the Council in the event of a further data breach, are completed first

Progress

The Enforcement Notice Action Plan contains 41 actions which are required to implement the nine recommendations. The ICO required the Council to implement the recommendations within 3 months, however, in some cases, this was impossible. Nevertheless, the Council has provided to the ICO a copy of the Action Plan, showing the status of each action, and current position.   A summary is provided as **Enclosure 1** to this report.

It is not necessary to refer to all the outcomes of the Enforcement Notice, however, in order to demonstrate how the assurance capability of the Council has improved, three issues are highlighted.

Data Security Incidents – Compliance With Policy

The Council already had robust and mature mechanisms for identifying, containing and reporting data security incidents as well as scoring the severity of those incidents. Compliance with the Council's Policy on Security Incidents is monitored. This means that the first recommendation of the Enforcement Notice is met.

Policy Management and Compliance

A suitable system to ensure that policies related to Information Governance are current, updated, readily available, and capable of providing suitable corporate reporting, was identified by the ICO in 2011 as an area for improvement. In 2015 the Council released funding for the acquisition of such a product.

The procurement process has been completed and the Council has now signed a Software Licence Agreement to acquire an appropriate system, together with e-learning opportunities. An Implementation Plan is currently being devised.

There will be a pilot involving a number of corporate services which are ensuring that all key policies are being updated, on an agreed template, and that executive summaries are also being devised. This will be available to all staff (and Members), with individual Services (and named individuals) being responsible for updating policies at certain key intervals.

The concept of “click to accept” (confirming that a policy has been read and understood) will only be utilised for certain key policies.

The CIGB hope that this product will be perceived as a useful repository for staff to access up to date policies across all corporate services rather than just an enforcement tool. There will be opportunities to extend the system at a later date, within Services, and individual teams, to share key documents that are relevant to their work.

Clear-Desk Audits

It is important that the information about people which Council staff need to use in the course of their duties is not left lying about when it is not being used, rendering it vulnerable to inappropriate access. The Council now has a clear-desk and clear-screen policy, which is monitored by the Heads of Service undertaking unannounced walk-around audits. These audits are monitored by a performance indicator; together with a number of other performance indicators relevant to information governance.

In conclusion, the CIGB will continue to monitor the actions which are underway on the current Action Plan, until they are completed. Thereafter the work will be re-prioritised. Until then the Policy Management System is the priority. We see this as the lynch pin for defending the Council in the event of any further reportable data breaches. The new system will be called The Policy Portal.

Enclosure 1

1. Data protection KPI's and measures are monitored and acted upon (including the number and nature of information security incidents)	Data protection KPIs are now in place and reported.
2. There is a mandatory data protection training programme for all staff (including new starters) and refresher training on an annual basis	There is a mandatory data protection training programme in place and the Council is looking to develop an e-learning package.
3. Completion of any such training is monitored and properly documented	Completion of training is now monitored and properly documented. The Council is currently discussing the implementation of a policy acceptance system with its service provider.
4. Policies (including the Records Management Policy) are being read, understood and complied with by all staff	The Council is currently discussing the implementation of a policy acceptance system with its service provider and, in addition, has undertaken a manual sign-up process to provide assurance.
5. Information is backed up to an external server on a daily basis	This is now done.
6. Back-ups are tested periodically to ensure that they have not degraded and that information is recoverable	This is now done.
7. Physical access rights are revoked promptly when staff leave and periodically reviewed to ensure that appropriate controls are in place.	The issue of access rights is being considered as part of a business re-engineering of the starters and leavers process which is being undertaken to provide assurance in this area.
8. The lack of adequate storage solutions for manual records is addressed	This is now addressed, with the Council's Corporate Information Governance Board retaining oversight of departmental record action plans.
9. Consistent and regular monitoring is undertaken to enforce the clear desk policy	This is now in place and monitored by a performance indicator.