Audit Committee – 12th September 2018

Report in absentia (John Worts – Information Security Team Leader)

(Responses in Red Font)

Recommendation 1: Framework to be implemented for conducting Privacy Impact Assessments in line with the guidance on such processes contained in GDPR (Priority 2).

Recommendation

The Council should develop a privacy by design approach to working and embedding the appropriate technical, administrative and physical safeguards required to comply with GDPR.

The Privacy Impact Assessment (PIA) should be embedded within Project management framework and risk management process.

For any new projects, a PIA should be undertaken to establish the potential impact on data protection/GDPR compliance.

Observation

The Council has not implemented a framework to allow them to identify instances where a privacy impact assessment would be required and how this would be performed in the event that an assessment should be undertaken.

Without implementing a framework for conducting privacy impact assessments, there is an increased risk that the Council will fail to comply with GDPR requirements regarding Data Protection by Design and Data Protection Impact Assessments. This in turn could result in breaches of the new Act and ensuing litigation and reputational damage.

The Council has carried out one off PIA's, but there is not a specific process in place for officers to carry out.

Responsibility: Information Security Manager / Innovation & Improvement Team Leader

Management response / deadline: The Data Protection Impact Assessment was made live in the Project Management Framework on 3/9/18. It will also be made live as part of the procurement and standing orders w/c 10/9/18

Recommendation 2: All staff to complete mandatory training (Priority 2).
Recommendation

An appropriate process should be introduced to capture all staff that have undertaken GDPR Training.

It should be ensured that all staff have completed Mandatory GDPR training as soon as practicably possible.

Observation

Staff GDPR training figures were provided at the time of the audit from the HR system, the DPO. This showed that although over 700 staff work at the council, but only just over 400 were shown on table sent.

As a result:

 A significant number of staff have not completed the mandatory training and/or

 The training statistics on the HR system are inaccurate.

Responsibility: HR and Information Security Manager

Management response / deadline: Note the figures (for 1 August 2017 to 30 July 2018) for Forum staff attending were 483. The discrepancy lies only with mainly manual working / outdoor working staff from Cupid Green attending. We will try to obtain the figures for Cupid Green Staff, Deadline by 31/10/18.

Recommendation 3: Scope for the Incident Management Policy to be updated with a flowchart to help staff to understand processes to follow in the event of an incident (Priority 3). Recommendation

The incident management policy should be updated and a flowchart attached as per the data breach policy, helping and enabling staff to effectively detect, report and investigate a personal data breach.

Observation

There is a Data Breach policy in place and accessible via the intranet. There is also a workflow document to help staff understand what to do in the event of a breach.

There is also an IT incident management policy for staff to follow in the event of an IT/virus failure.

Both policies have similar messages for staff, and the data breach policy has an easy to read workflow document which (in the event of an incident) staff could easily apply.

It was felt that it would also be useful for the incident management policy to be updated with a workflow diagram to enable staff to follow the process more clearly.

Responsibility: ICT in conjunction with Information Security Manager

Management response

Agreed – by 30/9/18 – John Worts to meet with Service Desk Team Leader (ICT). Note: The ICT incident workflow is already included in the Personal Data Breach Workflow – so just needs separating out to form the start of the ICT document.