AGENDA ITEM:

SUMMARY

Report for:	**Audit Committee**
Date of meeting:	**12th February 2014**
PART:	**1**
If Part II, reason:	

Title of report:	**Information Security Update**
Contact:	John Worts
Purpose of report:	1.To provide Audit Committee a general update on Information Security matters – particularly in relation to PSN and recommendations from ICO 2.
Corporate objectives:	Dacorum Delivers
Implications: 'Value For Money Implications'	<u>Financial</u> Potential costs involved in undertaking DBS checks for wider range of staff commencing 2014-15 Nominal costs are £25 for basic disclosure using Disclosure Scotland (Criminal record checks). <u>Value for Money</u> Cannot quantify – but may mitigate risk of fines from ICO (can be up to £500,000) and mitigate risk of disconnection from Government services (Revenues & benefits processing)
Risk Implications	
Equalities Implications	
Health And Safety Implications	None

Consultees:	
Background papers:	None
Historical background *(please give a brief background to this report to enable it to be considered in the right context).*	Derived actions from PSN work plan and Information Commissioners office recommendations.
Glossary of acronyms and any other abbreviations used in this report:	PSN – Public Sector Network Coco – Code of Connection GCSx – Government Secure Exchange ICO – Information Commissioners Office

Security Brief – Audit Committee
12th February 2014

Public Sector Network (PSN) Compliance

The Council successfully achieved PSN compliance from the Cabinet Office on the 27th January this year, following extensive hard work by the ICT teams (notably Dave Chamberlain, Ian Swinton, Darren Kemble and Kevin Bradley) and the Information Security Team Leader.

We have to annually reassure the Cabinet Office that our security measures are sufficiently robust and secure in order to continue receiving essential information from Government Departments and other organisations, such as the NHS for example. This information is necessary to enable us to carry out some of our services, such as the processing of Benefit claims. It is vital that we are able to communicate securely with Government Departments and other public organisations using our secure email addresses.

The work plan covers organisational, technical and physical security controls included in a 'code of connection' document (CoCo)

As a result of the compliance – there will have to be changes to the way we work in future in order to mitigate the risk of security breaches.

Some of these include;

1. The use of 'managed' devices to access the Council's network remotely via Dacorum Anywhere or other methods. Managed devices can include PC's, laptops, and phones. Managed devices are those authorised for use by the Council to staff and members. Unmanaged devices such as home PC's may pose a risk from insufficient malware protection, patching and other family members having unauthorised access to PROTECTED or RESTRICTED information.

2. A restriction on the use of encrypted USB sticks. The Dacorum Anywhere facility for home or remote working removes the requirement to store personal or confidential sensitive information on our encrypted USB sticks.

If you are storing personal or confidential sensitive information on an encrypted USB stick you must remove it immediately. The encrypted USB sticks must only be used for storing the Council's Emergency Plan and other documents related to emergency planning and business continuity.

3. There will be a requirement to carry out Disclosure and Barring Service checks on staff that use some of the secure government services. This extends in 2014 to all staff using a 'gcsx' or secure email account, and from

2015 to all staff on a PSN connected network. There will be a small cost (per person) to carry this out and discussions are underway with HR to determine how best to manage this process.

As a result of remedial work, following on from the IT Health Checks and penetration tests performed by an external company, all of the Critical and High vulnerabilities have been addressed by the ICT team.

Work will start in April in readiness for our next submission (27/6/13) to cabinet office.

External Sites and Suppliers

The Information Security Team Leader is currently reviewing access to our network by our systems providers. The review is called accreditation, and involves checks on security compliance, or ISO27001 certification, nominated staff checks, and equipment assurance (Patching and Anti-virus / Anti Malware measures). The type of remote access is now being limited to ensure that administrative privilege is only given to suppliers on request to the ICT Helpdesk. Administrative access is disabled by default.

A register of suppliers has been created on SharePoint, which will hold the evidential documentation for each supplier. More will be identified throughout 2014.

ICT Policies

From Q1 2014-15 the Information Security Team Leader will be carrying out a series of spot checks in random departments to ensure that staff have read and signed acceptance of the Councils Information Security and Information Management Policies.

ICO Recommendations and follow up

Further to the advice given to the Council following the Grove Hill Pavilion (2012) and Bennetts End Playground (2011) incidents, we now have in place, ‘zero client’ devices at all of the adventure playgrounds. These devices are fitted with a network cable, monitor port only. There is no storage on the device forcing staff to use Dacorum Anywhere to access their information securely.

The Council is also undergoing a major reduction in paper volume, through digitisation (into the Northgate document management system), or destroyed in accordance with the Council’s retention policy. There has been a lot of education over what constitutes confidential waste. The material is available to staff through SharePoint and there are flowcharts adjacent to the locked confidential waste bins.

There will be another round of disposal days during March with publicity, and most services now have a regular slot weekly for this. (Legal Governance – every Monday from 3.00pm)

A spot poll revealed that most staff are now using confidential waste for most items with the exception of empty envelopes and public domain training material.