REPORT TO:	Corporate Policy & Resources Policy and Performance Board
DATE:	29 October 2013
REPORTING OFFICER:	Strategic Director Policy and Resources
PORTFOLIO:	Resources
SUBJECT:	Security – Corporate Technology Services
WARDS:	Borough-Wide

1.0 PURPOSE OF THE REPORT:

1.1 At the last meeting of the Board, Members asked for an update of ICT Security within the Council's activities. This report provides an update of activities completed and planned and highlights the importance of security in the management and delivery of council services.

2.0 RECOMMENDATION:

(1) That the report be noted; and

(2) a further update be provided in 12 months' time.

3.0 SUPPORTING INFORMATION:

3.1 The Council manages a wide range of personal information relating to employees, businesses, external organisations and adults and children in the community both within and outside Halton.

Inappropriate access to information can have severely adverse effects on individuals or organisations if it falls into the wrong hands. The Council has a statutory as well as common law duty of care to ensure that all reasonable steps are taken to safeguard and secure the information it manages and processes.

ICT Services has designed an approach towards security in such a way that ensures the Council operates within its legal obligations while also enabling front line staff to deliver services in the most efficient and appropriate ways.

3.2 Security Assurance Activities

A range of activities has been delivered to ensure that the Council is discharging its duty to provide ongoing security and are detailed below:

Awareness Training – all employees were required to undertake on-line security awareness training in May 2013. There is an induction session for all employees which includes a session specifically on ICT Security.

Policy Development – A range of policies have been developed that clarify how services can operate while complying with the Law. These Policies are available to all staff and are reviewed annually.

Procedures - important procedures such as the recruitment and termination processes are being reviewed to ensure that the Council complies with the Baseline Personnel security Standard.

Governance – the Council has an Information Management Group that consists of representatives from directorates, Legal, HR and ICT services. The group reports to the ICT Strategy Group, and Senior Information Risk Owner (Strategic Director, Policy & Resources) who is ultimately responsible for the Council's Security arrangements.

Technical Controls – the way the ICT Systems are implemented and designed addresses the various security controls that the Council must comply with. There are many technical controls that are in place including:-

- Anti-Virus and Anti-Malware
- Internet Filtering (e.g. Payday loan sites)
- e-Mail filtering (preventing Spam and malicious e-mail attacks)
- Firewalls preventing external access to the Council's systems
- Laptop encryption (ensuring that if a laptop is stolen/misplaced, the data on it is protected)

External Testing - As well as designing systems in secure ways, the Council has several external tests undertaken every year to ensure that the Council's systems are secure, these are known as Penetration Testing, as they provide assurance that unauthorised access is prevented from outside the Council (e.g via the Internet or by "hacking" into our ICT networks in Council buildings).

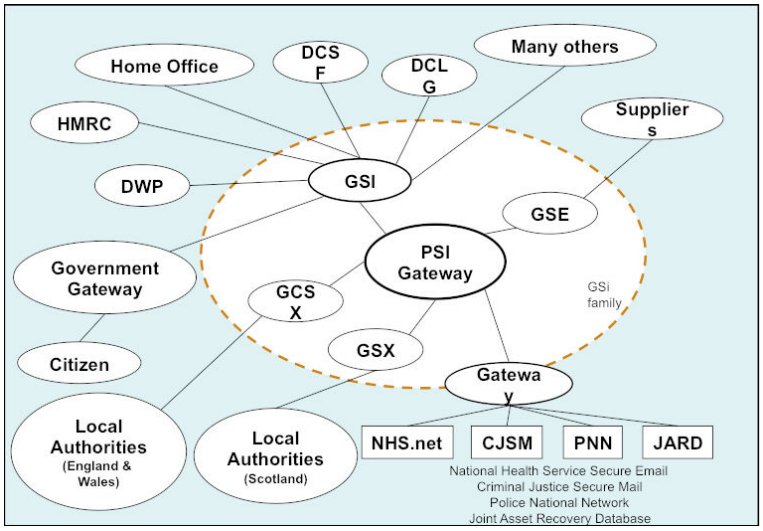
External inspection – there are a number of external organisations that require assurance that the Council is operating in a secure and compliant way. In addition to the regularity audits undertaken by Internal Audit and the annual External ICT Audit review by Grant Thornton, there are also annual reviews undertaken by A4e, Ingeus and Deloitte (for Halton People into Jobs).

3.2 Public Sector Network (PSN)

For the last 12 months the Council has been working on the transition from Government Connect Secure Extranet (the old GCSX process that has been the standard over the last 6 years) to the new Public Services Network (PSN).

The Public Services Network aims to substantially reduce the cost of communication services across UK government and enable new, joined-up and shared public services for the benefit of citizens. PSN aims to create one Government network, based on industry standards, potentially a more open and competitive ICT marketplace at the heart of the UK public sector.

The diagram below depicts how the government see this interconnect or hub may work with all agencies connecting securely thus enabling in theory the simpler transfer of data. The Council is using this network to its advantage and is working towards becoming a supplier of services over the PSN.



The Council has also put in place a "GCSX interconnect" allowing for our new Public Health Team to connect to the services it needs. The transition to PSN will allow for this to continue and develop as this area evolves and the authority becomes more involved within this area through the Public Health Team and the Clinical Commissioning Group.

The Council completes an annual ICT Security submission to the Cabinet Office which is assessed by GCHQ. If the Council fails this annual assessment, Central Government could prohibit Halton from being a part of the PSN, which would severely impact some key services such as Benefits and Public Health and have a direct impact on front line services.

3.3 **Payment Card Industry Data Security Standards (PCIDSS)**

As the Council accepts payments via various methods such as online, kiosks, and by telephone there must be compliance with the Payment Card Industry (PCI) standard. The Council must complete an annual assessment to provide the Banking Industry with the assurance that the Councils security systems are in place to prevent fraud.

3.4 **Business Continuity Planning**

A key part of ICT Security is ensuring that the Council can continue to operate in the event of an adverse event. Business Continuity Planning is the process, whereby contingency plans are developed to ensure that the Councils key operations can continue to be provided with limited systems availability.

Business Continuity and Disaster Recovery plans are continually reviewed and updated. Current projects are being worked on to ensure that service areas identify what priority systems they have and also what continuity plans are needed to ensure service delivery can take place if a significant adverse event did happen. Business Continuity exercises have been recently undertaken by each Directorate.

3.5 **ISO 27001 – International Security Standard**

As a result of the requirement for high standards of security and the need for the Council to demonstrate a recognised level of security to external organisations, the Council is now working towards compliance with ISO27001. This is a recognised international standard of information system security management. In order to comply with the standard there will be new policies and processes introduced across the council to maintain the focus on information security.

4.0 POLICY IMPLICATIONS:

4.1 It is imperative that the Council maintains high standards of information security to ensure that it retains the confidence of those whose information it retains and those organisations it shares information with.

5.0 IMPLICATIONS FOR THE COUNCIL PRIORITIES:

5.1 All council services are subject to security compliance in many ways from the core corporate compliance staff as users of technology within the authority are required to operate within, to legislative and practice requirement in many

of the areas the ICT Service supports and manages devices, data systems, solutions and applications.

5.2 **Children And Young People In Halton**:
The compliance with security and data regulations are critical operational requirements for the delivery of what are essential services. Compliance is carefully managed and monitored through the ICT teams, together with the management and teams within this directorate.

5.3 **Employment And Learning Skills Within Halton:**
As noted within the body of this report service contracts such as A4E and Ingeus (Halton People into Jobs) are supported by the ICT team and failure to comply in this area would result in the loss of such services and income.

5.4 **A Healthy Halton:**
As noted within the body of the report personal information and data sets are critical aspects of the Council's security focus and with the ever-increasing involvement within social care and public health, ICT security and corporate data security becomes an increased focus and requirement for the delivery of efficient services.

5.5 **A Safer Halton:**
As noted within the body of the report personal information and data sets are critical aspects of our security focus and with the ever-increasing involvement with partner agencies means that data security becomes an increased focus and requirement for the delivery of efficient services.

5.6 **Halton's Urban Renewal:**
There are no specific implications for this Council priority.

6.0 RISK ANALYSIS:

6.1 Although a considerable amount of activity relating to IT security, technology related in the behavior of employees with access to data is also crucial.

6.3 The Council has a Statutory and Common Law requirement to implement secure and safe ways of working

6.4 Risk is mitigated within these areas through the use of training, from the employee induction stage and continuously throughout the organization. Regular updates and staff briefings take place which remind employees of the importance of information security and of their own personal responsibilities.

6. 5 As the technology being used is changing from "traditional" computers such as Laptops and Desktops to a new world of mobile phones and tablet

devices, the Council needs to ensure all information held is managed and protected. This means a new view of security is needed, and accordingly, ICT Services are looking towards ways to protect the Council from “Data Loss” and “Mobile Device Management”.

7.0 EQUALITY AND DIVERSITY:

7.1 There are no equality and diversity issues relating to this report.

8.0 LIST OF BACKGROUND PAPERS UNDER SECTION 100D OF THE LOCAL GOVERNMENT ACT 1972:

8.1 All supporting papers are available from within the authorities Intranet.