REPORT TO:	Business Efficiency Board
DATE:	18 November 2015
REPORTING OFFICER:	Strategic Director, Community and Resources
PORTFOLIO:	Resources
SUBJECT:	Information Governance Annual Report 2014/15
WARD(S)	Borough-wide

1.0 PURPOSE OF THE REPORT

1.1 To present the Information Governance Annual Report for 2014/15 to the Business Efficiency Board.

2.0 **RECOMMENDATION: That the Board note the contents of the Annual Report for 2014/15.**

3.0 SUPPORTING INFORMATION

3.1 The Council's Information Governance (IG) function forms part of the responsibilities of the IG Team, Service Improvement Division within ICT Services.

Improving information governance has been a key priority for the Council since 2010/11 with the introduction of corporate information governance support within ICT Services.

In response to these challenges the Information Governance Group was introduced to look into information governance and information security and how best to move this forward in the Council.

The IGG meets every 6 weeks and supports the role of the Senior Information Risk Owner - SIRO.

3.2 IG is a key component of good governance in any organisation and consists of several aspects:

- Data Protection & Privacy
- Freedom of Information
- Information Security
- Information Sharing & Confidentiality
- Information & Records Management
- Information Quality & Assurance

IG has continued during 2014/15 to support senior managers and service delivery managers with the management of their information governance arrangements.

3.3 This is the first annual report to the Business Efficiency Board on Information Governance and contributes to the Council's assurance framework and good governance.

3.4 There are a number of pieces of legislation and good practice standards that govern the IG arrangements of the Council. The work of IG is primarily based on the requirements of the Local Authority Data Handling guidelines, ISO27001 (standard for information security), Data Protection Act 1998, Freedom of Information Act 2000 and Environmental Information Regulations 2004.

The Local Authority Data Handling Guidelines (stated above) recommend that each local authority should appoint a Senior Information Risk Owner (SIRO). The SIRO should be a representative at senior management level and has responsibility for ensuring that management of information risks are weighed alongside the management of other risks facing the Council such as financial, legal and operational risk. At Halton the nominated SIRO is the Strategic Director - Community and Resources. The Divisional Manager for Service Improvement in ICT Services acts as the Deputy SIRO.

3.5 **Information Rights**

Information rights is a collective name for 3 main pieces of legislation in respect to public sector information, these are:

Data Protection Act 1998 – looks at personal information relating to individuals
Freedom of Information Act 2000 – encompasses any information held by the Council
Environmental Information Regulations 2004 – information with an environmental impact

The IG Team has played a key role in providing assurance that the Council complies with information rights legislation in 2014/15. IG advises on the application of relevant exemptions in respect to requests received under information rights legislation.

IG also plays a prominent part when the Council receives a subject access request (someone requesting their personal information) or a request to access social care records, e.g. a parent asking to view the contents of their child's records. The Councils Data Protection Officer (Divisional Manager for Service Improvement) gives guidance on what records should or should not be released under the Data Protection Act 1998.

IG completed a review of the administration of Freedom of Information (FOI) requests in 2010/11. This review identified that the administration of FOI requests should be undertaken in one place therefore a decision was made to transfer the FOI function fully to IG to ensure FOI support is given from one area.

3.6 Security Incident Management Investigations

IG investigates all instances of alleged data breaches that are identified and referred to them. A data breach can cover a number of different incidents from a member/employee reporting a lost laptop to confidential/sensitive information being communicated to an unauthorised and/or incorrect recipient.

Following the implementation of the new ICT Directorate structure in October 2010, the Divisional Manager for Service Improvement instigated a procedure for formally recording alleged information breaches received and investigated. Before October 2010 possible breaches were investigated but recording of these was not formalised / consistent.

Between 1st April 2014 and 31st March 2015 there were 12 reported instances of possible data breaches. IG investigated all of these and confirmed that 1 data breaches had occurred and was reportable to the Information Commissioner. For each of these incidents the SIRO and IG agreed actions with the relevant management team to minimise the impact of the incidents on the customer and the council and to reduce the possibility of a similar data breach in the future.

The Information Commissioner’s decision in relation to the breach reported to them was that no further action would be taken against the authority. As part of that decision, the Information Commissioner emphasised that the authority’s commitment to introduce mandatory data protection training should be implemented as soon as possible.

3.7 Data Protection and Privacy

Information Governance/IT Security Awareness Week took place during October 2014 including daily Intranet homepage articles linked from the intranet news ticker, In Touch and Team Brief articles. Also undertaken

Fax Policy published

Data Quality and Corporate Strategy published

Freedom of Information Policy reviewed and published
Records Management Policy reviewed and published

Following a review of the Caldicott (is a set of principles that health and social care organisations use when reviewing the use of client information) and Data Protection guidance, including Caldicott Guardian Roles, Caldicott Staff Guide, Protecting Confidential Data Best Practice, Telephone Safe Haven, Email Good Practice, all documents have been published.

Office Audits have been completed and Operational Directors have been provided with reports for their areas.

3.8 Freedom of Information

Freedom of Information E-Learning courses are available for any staff involved in the handling of such requests and a review of the modules is due.

Statistics are produced at end of each quarter for the IGG and circulated to all Strategic Directors and Operational Directors. FOI Stats for the year ending 31st March 2015 are below.

Directorate	**Deadline Date Met**		**Grand Total**
	No	**Yes**	
Policy & Resources	28	565	**593**
Children & Enterprise	25	190	**215**
Communities	38	178	**216**
Grand Total	91	933	**1024**

3.9 IT Security

The Council is now considering gaining ISO27001:13 certification in which Security and Policy has been working towards in the background for a number of years in terms of good practice when documenting policies and procedures, as well as ensuring the Council complies to the cabinet office rules and internal and external audits. There are external contracts that Halton Borough Council have been awarded which specifically require compliance to ISO27001 conditions. Such contracts bring in money to the Council.

The IGG allows for the vast amount of policies for gaining ISO27001:13 to have a formal review and approval process. The IGG is the first step for approval before ICT Strategy Board consideration and union consultations where necessary.

The following policies have been completed and the majority have already been approved via the approval process. Meetings have now been taking place with the Records Management Unity - RMU to ensure the procedures for the RMU now meet ISO27001:13 as well as the policies.

Information Security Policy
Organisation of Information Security Policy
Mobile Computing and Teleworking
Human Resource Security Policy
Asset Management Policy
Acceptable Use Policy
Removable Media Policy
Information Classification Policy
Access Control Policy
Cryptography Policy
Physical and Environmental Policy
Clear Desk and Screen Policy
Operations Policy
Backup Policy
Change Management Policy
System Acquisition, development and maintenance Policy
Supplier Relationships
Information Security Incident Management Policy
Information Security aspects of Business Continuity Policy
Compliance Policy

As well as ISO27001:13 compliance in terms of policies and procedures the actual project documentation is being created which includes the business case for approval, statement of applicability which is a gap analysis of where we are and where we need to be to gain certification and most importantly the correct scope of the project.

ELearning for IT Security and Information Governance has also been upgraded by Security and Policy and Information Governance in partnership for all users to complete across the council so they can become more educated on the rules and legislation they need to comply with.

3.10 **Information Sharing**

The production of Tier 2 Information Sharing Agreements by all divisions with third parties is an on-going area of work and it is hoped to have a full library of all such agreements that exist across the Council in the future. The Information Sharing Agreement Library holds the agreements so far recorded and made aware to the IG team.

3.11 **Information Quality and Assurance**

IG Toolkit – Halton Borough Council are part of the 5 Borough's partnership with Health and other partners. An essential requirement for the Council is to be able to connect to health systems and in order to connect we are required to complete an Information Governance Toolkit assessment which is an online assessment consisting of around 29 attainment levels. Extensive work is undertaken by the Information Governance Team and the Security and Policy Team to complete the assessment by March of each year. Halton has completed and submitted the assessment for version 12 (year ending March 2015) and confirmation of successful submission has been received.

3.12 **Current ongoing work areas**

A full review of Council's Information Governance requirements is being undertaken which includes:-

Information Governance Toolkit Assessment for 2015/16
Information Governance Handbook
Information Sharing Policy
Records Retention Policy
E-Learning modules for FOI and Subject Access
SIRO/IAO Guidelines
Training as follow up to office audits
External data flow analyses
Work towards incorporating IG in corporate projects at outset

A full review of Information Governance requirements for schools is ongoing which includes -

Model School Data Protection Policy
Model Schools Policy for Disposal of Redundant ICT equipment
Model Schools Data Quality Policy
Model Schools FOI Policy
Model Schools Subject Access Policy
Model Schools Publication Scheme
Model Schools Policy for Data Security
Heads Guidance - Data Security
Staff Guidance - Data Security
Network Managers Guidance - Data Security
Model E Safety Policy
Model School Policy - Records Management
Privacy Notice for Schools – short version
Privacy Notice Primary aged children
SIRO IAO Guidance - Data Security
Acceptable Use Agreement Staff Governors Visitors
Primary Pupil Acceptable Use Agreement
Secondary Pupil Acceptable Use Agreement

Press and Publicity in Schools

3.13 **Data Security**

All laptops with access to the network have been encrypted. This is provided by McAfee endpoint encryption. The use of non-Council owned laptops for person identifiable data is not permitted. There is also a reduced amount of users with outlook web access due to the potential of users accessing emails on their personal devices at home and saving personal / sensitive information to their own devices which will not have the same security controls.

Machines are also locked down centrally so users can only access what they need to access and they cannot install software without the need of a member of ICT Services. There are processes in place to test any software off the network before ICT allow software to be installed, this is to reduce the risk of introducing viruses.

The SIRO is kept informed of emerging issues via copies of the minutes of the Information Governance Management Group

3.14 **Training**

All staff received an email from the Chief Executive and all DMs have received an email regarding the E-Learning training module for "IT Security and Information Governance" encouraging all staff to complete the course. The course helps staff gain an understanding of the principles of IT Security and information governance. E-learning reports are being monitored. Further tailored training has been arranged with Adoption and Fostering Services staff and guidance for manual workers has been introduced for those workers who do not use IT equipment. Manual workers are asked to sign to confirm they have read and understood the guidance.

3.15 **Information Asset Register**

We are moving towards all directorates having an Information Asset Register in which all the Council's Information Assets have been recorded and are being assessed for risk. This is part of the activities involved in producing the Information Asset Owners Guidance.

3.16 **Conclusions for 2014/15 and looking forward to 2015/16**

The IG team has like all areas of the Council been affected by reducing resources during 2014/15. There have also been increased pressures in 2014/15, primarily due to increased public awareness of their information rights and an increase in the number of alleged data breaches reported.

There have been a number of initiatives that had previously been planned by IG that were progressed in 2014/15 with an expectation of full implementation in 2015/16. Key initiatives that have been progressed include:

a) Information Governance Handbook
b) Information Asset Owner Guidance
c) Information Life Cycle Policy
d) Information Sharing Policy
e) Records Retention Policy
f) E-Learning modules for FOI and Subject Access
g) Developing training and awareness

Training and awareness underpins all information governance requirements and aims to equip employees with the necessary skills/knowledge to comply with information legislation and good practices.

IG intends to build on the progress made in 2014/15, and that of previous years, to continue to meet the current and future needs of the Council.

An annual report will now continue to be presented to the Business Efficiency Board providing an update on information governance and activity of the team during the year.

4.0 POLICY IMPLICATIONS

4.1 The IG process has developed and maintains policy and guidance covering all relevant aspects of Information Governance

5.0 FINANCIAL IMPLICATIONS

5.1 The major impact would be an ICO fine resulting from major data breach. Council had a reportable data breach in June 2013 and the ICO imposed a fine of £70,000.

5.2 The work being undertaken by Council as outlined in this report is to minimise the risk of a further data breach that results in an ICO fine.

6.0 IMPLICATIONS FOR THE COUNCIL'S PRIORITIES

6.1 Not applicable.

7.0 Children & Young People in Halton

7.1 Not applicable.

8.0 **Employment, Learning & Skills in Halton**

8.1 Not applicable.

9.0 **A Healthy Halton**

9.1 Not applicable.

10.0 **A Safer Halton**

10.1 Not applicable.

11.0 **Halton's Urban Renewal**

11.1 Not applicable.

12.0 **RISK ANALYSIS**

12.1 The Council –

Acknowledges the importance of protecting customer's privacy and strives to comply with all relevant legislation and best practice to achieve this.

Values the personal information entrusted to it and makes sure it respects that trust.

Goes further than just the letter of the law when it comes to handling personal information and has adopted good practice standards.

Keeps personal information to the minimum necessary and deletes it when it's no longer required.

Has effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands.

Provides training to staff that handle personal information and treat it as a disciplinary matter if they misuse or don't look after it properly.

Regularly checks that it is living up to those commitments and reports on how it is doing.

13.0 **EQUALITY AND DIVERSITY ISSUES**

13.1 Not applicable.

14.0 **LIST OF BACKGROUND PAPERS UNDER SECTION 100D OF THE LOCAL GOVERNMENT ACT 1972**

There are no background papers under the meaning of the Act.