Key Decision Required:	**No**	**In the Forward Plan:**	**No**

CABINET

12 DECEMBER 2014

REPORT OF PLANNING AND CORPORATE SERVICES PORTFOLIO HOLDER

A.7 INFORMATION GOVERNANCE

(Report prepared by Judy Barker and John Higgins)

PART 1 – KEY INFORMATION

PURPOSE OF THE REPORT

To provide Members with an update on the work carried out by the Council to improve its arrangements for the management and security of information.

EXECUTIVE SUMMARY

Information is one of the key resources of the Council. It is critical to the delivery of services and the way in which it is held and used (processed) is subject to legal requirements – the Freedom of Information and Data Protection Acts –Government IT security requirements and must be in accordance with the Council's Information Charter (Appendix A1).

Significant opportunities exist for Councils to use and share information both within their organisations and with partners to deliver joined up, more efficient and more responsive public services.

Information Governance is the term used to draw together all of the arrangements the Council needs to put in place to ensure that the information it holds is processed securely and in accordance with the law and also to ensure that it is used in an efficient way to deliver good public services and positive outcomes for the residents of the District.

Much progress has been made in drawing together and improving these arrangements which has involved officers from across the Council's services. The key elements are

- A Policy Group of key officers chaired by the Planning and Corporate Services Portfolio Holder.
- An operational group of officers involved in the various types of work involving information who work together to ensure our approach is joined up.
- A Corporate Information Security Policy.
- An annual programme of work to ensure we meet the ever increasing standards required to connect to the Government Public Services Network (PSN).
- Monitoring and reviewing of policies involving information – three major policies reviewed, two still to do.
- Extensive training for lead officers and more general training for over 50 staff on Data Protection.

- Revised and updated arrangements for handling Freedom of Information requests and a full update to the Council's published retention scheme.
- Active engagement (at an early stage) with the Whole Essex Information Sharing Framework (WEISF) which is being led by Essex County Council.

The six sections of the report set out the current position in relation to each of these areas of work.

RECOMMENDATION

That Members note the progress made and the work to be done in relation to the Council's arrangements for Information Governance.

PART 2 – IMPLICATIONS OF THE DECISION

DELIVERING PRIORITIES

The measures being undertaken by Tendring in respect of information governance contributes to the provision of excellent, sustainable services to everyone in the District by ensuring that the processing of information continues to meet security standards, and steps are taken to mitigate risks as they are identified.

FINANCE, OTHER RESOURCES AND RISK

Finance and other resources

All activities to improve the Council's information governance have been met from within existing IT budgets.

Risk

The steps taken are designed to remove or mitigate the risks associated with the processing and secure storage of information. Failure to do so would open the Council to potential non-compliance issues with the Data Protection Act, Freedom of Information Act, Public Services Network (PSN) Code of Connection and other associated legislation which could result in fines being levied by the Information Commissioner or as a result of civil action and the damage to the Council's reputation that could result should a security breach occur. In addition, should the PSN Code of Connection requirements not be met, continued use of the PSN would be removed or restricted causing a negative impact on the business needs and statutory functions of this authority.

The Council has a program of regular vulnerability audits under the Payment Card Industry (PCI) standards, IT network and scans, IT backup and disaster recovery arrangements and the compulsory annual IT Health Check and associated remediation plan required by the PSN. In addition it maintains and promotes a programme of training to ensure its officers continue to have the knowledge and skills necessary to handle information in a secure manner.

LEGAL

The proposals set out in this report are within the Councils powers.

OTHER IMPLICATIONS

Consideration has been given to the implications of the proposed decision in respect of the following:

Crime and Disorder / Equality and Diversity / Health Inequalities / Area or Ward affected / Consultation/Public Engagement.

PART 3 – SUPPORTING INFORMATION

BACKGROUND and CURRENT POSITION

1. Information Governance Framework

A new framework has been established in order to address the growing number of information governance requirements arising from the Public Services Network (PSN) Code of Connection (CoCo) and the ongoing need to continually improve our information security arrangements.

The new Corporate Information Security Policy (see section 3 below) recommended a number of information governance roles and responsibilities, thereby devolving routine operational changes arising from legislative and/or administrative requirements to the Corporate Director (Corporate Services) who will do so in consultation with the Planning and Corporate Services Portfolio Holder who chairs the new Information Governance Policy Unit (IGPU).

These groups are now well established and attended. The table below briefly describes their purpose and attendance.

Group	Purpose	Attendance
Information Policy Unit (IGPU)	Development and/or adoption of new policies, procedures and standards. Corporate Information Security Policy legislative and administrative changes through the Corporate Director delegated powers.	Chaired by the Planning and Corporate Services Portfolio Holder and includes: • Corporate Director (Corporate Services) • Data Protection Officer • Human Resources • Senior Information Risk Owner (SIRO) – role currently held by the IT Manager • Monitoring Officer • Data Protection Manager

Information Security Management Group (ISMG)	Annual review of polices, evaluation of exposure to risk and overseeing all info security related projects. Appropriate members of this group could also act in the role of security incident response / containment team with the addition of the Facilities & Emergency Planning Manager, the Corporate Communications Manager and the Corporate Director (Corporate Services).	Chaired by the SIRO and includes: • IT Security Officer (nominated) • Data Protection Officer • Freedom Of Information & Environmental Information Regulation officers • Operational Manager representative • Internal Audit

2. Public Services Network (PSN) Compliance and Migration

The Public Services Network (PSN) provides the Council with a secure link to central government, public sector partners and other government agencies. This secure link is increasingly required for a range of activities, sensitive or personal data sharing including daily sharing of Housing Benefit data / information between the Council's Housing Benefits team and the Department of Works and Pensions (DWP), access to the DWP Customer Information System (CIS) is dependent on it, Benefit Fraud investigations, electoral data for jury service, the police, etc.

This secure connection was originally provided via the Government Connect Secure eXtranet and was replaced in November 2012 by the PSN. Tendring achieved compliance with the challenging PSN Code of Connection (CoCo) (90+ control condition compliance statements) in August 2013 and migrated to the PSN infrastructure in January 2014 and was among the first 10% of public sector organisations to achieve compliance, despite the stringent additional security measures that were imposed.

It is estimated that initial PSN compliance/ certification cost Tendring District Council around £80,000 (2013/14) in unplanned network segregation costs, replacement/new hardware, specialist IT audit health check consultancy and significant internal resource commitments. It should be noted that our IT partner, Trinity, played a key role in helping Tendring achieve compliance.

Continued PSN connectivity is conditional on an annual compliance assessment which also demands a comprehensive IT security audit by an approved external company (CESG approved companies with accredited penetration testers qualified to assess HMG systems up to and including SECRET classification) and this took place during the week of 27 October 2014 in preparation for our next assessment in February 2015. It is expected that the security bar will again be raised generating additional works and further unplanned for and, as yet unknown, costs in order to retain connection.

The Government also implemented a new information classification scheme (GCS) in April of this year which replaces the previous Government Protective Marking Scheme (GPMS) which had been in place for many years. One of the requirements contained within the CoCo is to classify all emails and documents originating within our organisation. A project to address this issue has commenced and is scheduled for completion in late November 2014.

3. Policy Review

- **Information Security Policy**

  A new Information Security Policy was produced and adopted by HR Committee in February 2013 as part of the steps toward compliance with the PSN code of connection.

  The new policy consolidates and replaces our previous e-mail, intranet use and internet use policies for officers within its 'Conditions of Acceptable Use'. The Policy also includes a clearly worded 'dos and don'ts section along with a 'Personal Commitment Statement' for our GCSx (PSN) secure email users to complete. This has now been fully implemented and forms part of our successful PSN accreditation. The policy applies equally to officers and to members.

  The new Corporate Information Security Policy is intrinsically linked with the Essex OnLine Partnership (EOLP) model answer document which assisted the Council with its Code of Connection submission for PSN connection. Therefore adopting this policy and the corresponding model answer suite of cross-referenced documentation assisted the Council to achieve compliance without further significant additional resourcing which saved an estimated £6,000 consultancy costs (based upon 2011/12 GCSx costs). It is anticipated that this document will continue to serve us well in our next code of connection assessment in February 2015.

- **Monitoring Policy review**

  A full review has been undertaken of the Council's Monitoring Policy by the Information Security Management Group and a draft has been agreed by the Information Policy Unit.

- **Corporate Retention Policy**

  A project team, with representation from all departments and led by Katie Wilkins of Corporate Services Business Unit, were tasked with reviewing the Council's Corporate Retention Policy (last updated in 2004). This was a substantial piece of work and has resulted in a revised policy and accompanying Schedule document which details all organisational requirements with regard to document retention and storage. Adoption and compliance with this new policy is a key pre-requisite in the delivery of the Council's planned corporate-wide Electronic Document Records Management System (again, funded through the Strategic IT Investment Programme agreed by Cabinet in September 2013).

  The Schedule consists of four sections which detail specific functions for each department, the type of records that may fall within this function and the length of time the Council should hold the record before taking disposal or archive action. The four departmental sections are complemented with an overarching guidance document for the more generic principles that apply across the board.

  The importance of this work was recognised and approved by Management Team with the new policy being adopted in January 2014. The content of the document was also recently used to reinforce elements of the data protection training delivered to managers and senior officers. The policy will continue to be subject to regular review to ensure it remains fit for purpose.

- **Other Polices**

  There are two other policies yet to be reviewed. These are :-

  - IT Security Policy (currently at first draft stage)
  - Data Protection Policy (dependent on date of new EU Regulation)

4. <u>Data Protection Act (DPA) Training</u>

In October 2013 data protection representatives from each directorate /department attended a formal external training course resulting in all 6 attendees attaining a level 2 certification in The Principles of Data Protection (Data Control) with an average pass mark exceeding 90% - an excellent result.

Following discussion at the Information Governance Policy Unit, it was agreed that a new data protection training course for managers was required to ensure that the Council provided adequate training to its officers so that they understand both their personal and corporate responsibilities when handling personal information. This course complements the existing e-learning material that is available to all officers and members.

The course was developed by the Council’s Data Protection Manager and IT Trainer (Trinity) and has now been successfully delivered to 57 managers and nominated senior officers over 11 courses. The course has been very well received with an average satisfaction score of 6.4 out of 7. A mop-up session will be arranged for early autumn for the few who were unable to attend.

Online E-learning data protection training is available for members.

5. Freedom of Information (FOI)

- **Revised Publication scheme**

  After meetings between Legal Services and the Departmental Freedom Of Information Co-ordinators the Publication Scheme was fully reviewed and updated in line with the Information Commissioner’s Model Scheme. This is now fully up-to-date on the FOI Section of the Website.

- **Upgraded Freedom Of Information Recording System**

  Following a review of what was required by departments to record all requests for information and to provide both the departmental and corporate reporting tools necessary to accurately monitor and manage responses, a full review was undertaken of the FOI database application. A number of changes were identified and these amendments have all been completed and were implemented in January 2014. All departmental coordinators are now using the upgraded system.

- **Freedom Of Information Practitioner Training**

  The Legal Administration and Information Officer has now gained the nationally recognised Practitioner Certificate in Freedom of Information qualification.

- **Corporate Procedures for Handling Requests for Information**

  A range of document templates exist for handling enquiries. These have all been reviewed and updated and are now available to all departmental FOI Co-ordinators via the Intranet. This provides the opportunity for standard response text to be used where appropriate.

- **Handling Requests from Councillors**

  All departmental Freedom Of Information Co-ordinators have now been advised that if they receive any FOI requests from or in relation to Councillors then responses are reviewed by Legal Services prior to being disclosed. This is to ensure that responses are appropriate in relation to a Councillor’s public and private life.

6. WHOLE of ESSEX INFORMATION SHARING FRAMEWORK (WEISF)

Essex County Council’s Health and Wellbeing Board commissioned a task and finish project into how personal information could be securely shared across Essex in compliance with the legal requirements of the Data Protection Act and the guidance issued by the UK Information Commissioner as a minimum standard.

The first meeting of the WEISF Management Group took place on 1st July 2014 and was attended by representatives from the county council, local authorities, health, emergency services and the community and voluntary sectors. Tendring has been represented from the start.

The WEISF is to provide of a web based portal to host information sharing protocol templates which will be available for use by all members of the group. ECC intend to provide the portal with maintenance and updating being handled centrally by them.

Tendring District Council has signed up to the WEIF principles as an interested partner and John Higgins has been nominated to represent the Council at future meetings. A management board is currently being established to include a representative from each of the sectors to manage the project as it progresses. More information will be available once the terms of reference, membership, roles and responsibilities and costs have been finalised.

A recent information sharing funding bid for a grant of £2.7m from the Department for Communities and Local Government (DCLG) was made by Essex County Council, assisted by various partners and with Tendring District Council playing a key stakeholder role. Confirmation has been received that the Expression of Interest has been approved and a full business case is now being prepared for submission in early October; again, Tendring District Council is instrumental in driving this forward.

BACKGROUND PAPERS FOR THE DECISION

None

APPENDICES

Appendix A1 – Information Charter

Appendix A1

INFORMATION CHARTER

We need to handle personal information about you so that we can provide better services for you. This is how we look after that information.

When we ask you for personal information, we undertake to:

- ✓ make it clear why we need it;
- ✓ ask only for the amount of information we need;
- ✓ protect it and make sure it is only accessible to those who need to use it;
- ✓ only share information within our organisation or with other bodies where it is necessary and would be compatible with the purpose for which we collected it, or where we are required or permitted to do so by law;
- ✓ make sure we only keep it for as long as is necessary; and
- ✓ only make your personal information available for commercial use with your permission (for example on the edited version of the electoral register).

In return, to ensure that your information is correct and kept up to date, we ask you to:

- ✓ provide us with accurate information; and
- ✓ tell us as soon as possible if there are any changes to this information (for example a change in your address).

How to find out what information we intend to process :

The Data Protection Act 1998 requires the Council to notify the UK Information Commissioner how it intends to gather and process personal information. This information is made available via a public register.

The principal purpose of having notification and the public register is transparency and openness. It is a basic principle of data protection that the public should know (or should be able to find out) who is carrying out the processing of personal information as well as other details about the processing (such as for what reason it is being carried out).

The Council has two register entries:

Electoral Administration functions (Registration No. Z6205259); and

All other Council activities (Registration No. Z577148X).