REPORT TO THE MEETING OF THE EXECUTIVE 17 JULY 2013

PORTFOLIO: SERVICE DEVELOPMENT, IMPROVEMENT AND PERFORMANCE MANAGEMENT

REPORT FROM HEAD OF INFORMATION AND CUSTOMER SERVICES

SUBJECT: ICT SECURITY POLICY AND PRACTICE

1 DECISION BEING RECOMMENDED

1.1 To approve the updated Corporate Information Security Policy and Personal Commitment Statement.

1.2 To implement a standard approach to the use of IT by Members, as set out in paragraph 3.14 of this report.

1.3 To authorise the Portfolio Holder for Service Development, Improvement and Performance Management to approve a specific procedure note around Members' use of IT as set out in paragraph 3.15 of this report.

1.4 To authorise the Head of Information and Customer Services, in consultation with the Portfolio Holder for Service Development, Improvement and Performance Management, to implement a system of remote access to IT systems by officers should this be necessary once our IT security submission has been assessed by the Cabinet Office.

2 REASON/S FOR RECOMMENDATION

2.1 In running the business of the Council, we have to comply with the requirements of the Freedom of Information and Data Protection Acts, and the Code of Connection (CoCo) to the Public Services Network (PSN). We need to ensure transparency of operation and consistency of approach in how data is managed.

2.2 To achieve compliance there is a need for a standardised approach to the use of IT and electronic communications by Members, which will require Members to sign up to the Council's Corporate Information Security Policy.

2.3 It is also necessary to review how officers use IT when away from the office to ensure compliance with IT security requirements.

3 SALIENT INFORMATION

3.1 Each year the Council has to submit to the Cabinet Office an IT security assessment against the requirements of the CoCo to the government secure network. We submitted our last assessment in September 2012, in which we proposed a solution for Members' use of IT to achieve compliance. This

involved the cessation of the auto-forwarding of councillor@rochford.gov.uk emails to a Member's private email address (considered to be a security risk), with Members instead having to log in remotely to the Council's secure systems to view their emails. The implementation of this was delayed pending a positive response to the inspection.

3.2 The Cabinet Office has recently informed us that, due to work levels and a processing backlog, the 2012 inspection will not be assessed and, instead, we have to submit a new 2013 CoCo PSN assessment by September 2013. The Cabinet Office has stated that there will be a 'zero tolerance' approach to complying with this new regime.

3.3 Officers have been assessing the requirements of this new regime and working to ensure that our 2013 submission is compliant. As a result, our Corporate Information Security Policy, and associated documents, have been updated. The Policy and the Personal Commitment Statement are attached at Appendix A. All staff and Members will be required to sign up to the updated Policy once approved.

3.4 The associated documents referred to above are as follows:-

- Bring Your Own Device (Interim) Policy
- Clear Desk Policy and Procedure
- Guide to Email Management
- Guide to Passwords
- ICT Policies / Disciplinary Procedures
- Procedure for Gaining Access to Other Staff's Emails
- Procedure for Linking Portable Electronic Devices to the RDC ICT System
- Procedure for Moving Non Portable ICT Equipment
- Procedure for Reporting Information Security Incidents
- Procedure for Sharing Sensitive Data Securely with Third Parties
- Procedure for Taking Data Outside the Workplace
- Procedure for using RDC ICT Equipment Outside of the Workplace
- Procedure for the Installation of Software
- Procedure for using Mobile Technology Abroad

These are not attached to the report but are available for Members from the Head of Information and Customer Services on request.

Members Use of IT and Electronic Communications

3.5 It is clear from the CoCo requirements that the current practice of auto-forwarding a councillor@rochford.gov.uk email from a secure environment across the internet to a personal email address is not compliant. In addition, the Corporate Information Security Policy requires that data classified at 'Protect' or above must not be sent in emails across the internet.

3.6 Data is considered to be at 'Protect' or above if its disclosure would cause distress to individuals, cause financial or potential financial loss, facilitate improper gain or unfair advantage, prejudice the investigation or facilitate the commission of crime, breach statutory restrictions on the disclosure of information such as the Data Protection Act, or if it was provided in confidence. It covers most types of casework that contain the personal details of individual residents that should not be exchanged across the internet, and, potentially, also covers some business information leading up to decisions and the type of information contained in the 'purple' committee reports.

3.7 Currently one Member with a rochford.gov.uk email address has their emails auto-forwarded to Member Services to print out and put in the drop; one Member has no personal IT access; and one Member does not have an auto-forwarding arrangement due to concern about their private email address being made public. There are also occasions when Member Services are sent and asked to print out for the drop an email for Members. There are a number of issues associated with this practice, including:-

- Officers may get to see confidential / personal correspondence between Councillors that may include comments about other Officers / Members, etc.
- Officers may get to see political group communications intended for recipients only.
- Residents and others sending emails will not realise that they are being seen by people other than the addressee.
- There can be time delays between printing off emails and them being seen by the Member. Associated with this is the fact that the Member Services team cannot respond on behalf of a Member so a correspondent can be left wondering if a Member has seen an email or, even worse, think that the Member is not interested in their problem.
- Officers deciding whether an email should be printed off or not could lead to issues (many emails are only advertisements etc, but it is a judgement call).

This practice therefore needs to be discontinued.

3.8 The Freedom of Information Act (FoIA) provides that, in circumstances where information is held by another person on behalf of a public authority, the information is considered to be held by the authority for the purpose of the FoIA. The FoIA, therefore, applies to official information held in private email accounts (and other media formats) when held on behalf of the Council.

3.9 The Information Commissioner has issued guidance which states that information held in non-work personal email accounts (e.g. Hotmail, Gmail, etc.) is likely to be subject to the FoIA if it relates to the official business of the Council. All such information which is held by someone who has a direct, formal connection with the Council is potentially subject to FoIA regardless of whether it is held in an official or private email account.

3.10 The Information Commissioner specifically states that "in the local government context, there is a need to have a clear demarcation between Council business and work for individuals as their local representative."

3.11 Information is subject to the FoIA if it is held by a Councillor in their role as an agent or representative of the Council. This includes:-

- An Executive Member acting on behalf of the Council.
- Information received or produced by a Councillor acting as a representative of the Council.
- Any Member sending or receiving letters on behalf of the Council.

3.12 Official information recorded on mobile devices, including text messages on mobile phones or in any other media, can also be considered to be held on behalf of the Council in the circumstances outlined and so are also subject to FoIA.

3.13 The Information Commissioner's guidance states that "information on authority-related business should be recorded on the authority's record keeping systems in so far as reasonably practical. It is accepted that, in certain circumstances, it may be necessary to use private email for public authority business. There should be a policy which clearly states that, in such cases, an authority email address must be copied in to ensure the completeness of the authority's records. In this way, records management policies will make it easier for public authorities to determine whether information is held and to locate and retrieve it in response to requests. If the information is contained within the public authority's systems it can also be subject to consistently applied retention and destruction policies."

3.14 It is, therefore, proposed that a standardised approach to electronic communication be adopted for all Councillors as follows:-

(a) All Members to be provided with a councillor@rochford.gov.uk email address for Council business.

(b) The councillor@rochford.gov.uk email addresses to be made public.

(c) All Members to be provided with an iPad to view their emails and documentation. The iPad to have 'Good' software installed on it to ensure that emails are retrieved in a secure environment. Alternatively, Members will be able to log into the Council's network to retrieve emails at the Civic Suite. For District Members who are also County

Members it will be possible to auto-forward Rochford District Council emails to their County email address as the security levels are similar and the County Council has provided the equipment.

(d) Councillor@rochford.gov.uk emails to no longer be forwarded to a Member's private email address.

(e) Member Services to no longer print out or forward emails for Members.

(f) All Councillors to be required to sign up to the Council's Corporate Information Security Policy.

(g) The Council's iPad to only be used for Rochford District Council business within the terms of the Council's Corporate Information Security Policy.

3.15 Whilst Members will be required to sign up to the Council's Corporate Information Security Policy, it will also be necessary to have a separate document setting out in practical terms matters such as the definition of acceptable use and the requirement to take reasonable care of equipment supplied by the Council. This will be approved by the Portfolio Holder, in advance of the issue of the iPads.

3.16 The iPads will be used in the first instance for Members' emails. Once implemented, it will be possible to explore how Members can receive documentation, such as agendas and minutes, electronically. The proposed arrangements for this will be the subject of a report to the Executive in Autumn 2013.

Remote Access by Officers

3.17 There is currently some uncertainty whether the method by which officers have remote access to the Council's systems is compliant with the CoCo. Officers use their own home equipment with a 'cryptocard' to gain access, but this single layer of authentication is potentially deemed to be insecure.

3.18 Currently around 80 staff have remote access to the Council's systems, and this is a key element in business continuity and disaster recovery planning.

3.19 Officers have asked for specific clarification from the Cabinet Office on this point, particularly as only a limited number of staff need to access information across the PSN itself.

3.20 The response received from the Cabinet Office is that accessing any PSN services from any non-Council equipment is forbidden. This is clear and therefore the 4 staff who are homeworkers in Revenues and Benefits will have to be supplied with Council equipment. This will cost in the region of £1,800 to supply terminals, screens and keyboards.

3.21 In respect of other officers who work remotely but who do not access PSN services, the response from the Cabinet Office is as follows: "You may use an appropriately secured solution for accessing standard internal Rochford services but only if you can demonstrate that the users will not in any way present a risk to the PSN connection". It is believed that our current arrangements do meet this requirement and the intention is, therefore, to explain our current arrangements in the CoCo submission. It is a possibility however that the Cabinet Office will not approve our solution.

3.22 The options to enable the continuation of remote access by officers if the Cabinet Office is not satisfied with our current arrangements are as follows:-

- purchase of IT equipment (tablet, thin client unit or smartphone) for remote/home use; or

- purchase of specific software, called Ericom Blaze, that allows remote connection from non-RDC devices in a secure manner. This software is currently undergoing the accreditation process to be approved for use under the CoCo. If it does not receive accreditation this will not be an option.

3.23 This report, therefore, seeks approval for the Head of Information and Customer Services, in consultation with the Portfolio Holder, to implement the most cost effective solution to enable the continuation of remote access by officers, should this be necessary once the Cabinet Office have assessed our CoCo submission.

3.24 A 'Bring Your Own Device' (BYOD) policy and procedure is under development to govern how officers use their own equipment remotely for RDC business to take account of the emerging legislation in this area. An interim policy is currently in place. However, in order to ensure that full advantage is taken of the move to electronic documentation and the efficiencies that this can bring, it is proposed that the Senior Management Team are also provided with iPads.

4 RISK IMPLICATIONS

4.1 If we do not achieve compliance with the CoCo PSN there is a risk that the Council's connection to the government secure network will be removed. This would have implications for the continued effective operation of the revenues and benefits service which needs to exchange information with the Department of Work and Pensions. It would also impact on the ability to implement Individual Electoral Registration as this also requires access to the government secure network.

4.2 There is also a risk to the Council if personal data is not handled in accordance with legislation. There could be distress to a person whose data is mishandled, as well as reputational damage to the Council where a data protection breach has occurred. This could lead to loss of trust from the

general public about the organisation's ability to properly safeguard their personal information.

4.3 There can be financial consequences to the Council imposed by the Information Commissioner if the Council is found to have breached legislative requirements. The Information Commissioner has the power to impose fines of up to £500,000 for serious breaches of the Data Protection Act, as well as being able to serve enforcement notices. A number of Councils have been fined substantial sums for falling short of their responsibilities. Examples include Cheshire East Council, which was fined £80,000 when an officer sent sensitive data via his personal email rather than using the Council's secure email system. Since June 2011 the following fines have been imposed on Councils (numerous other fines have been issued to other public sector bodies and the private sector):-

- Glasgow City Council: £150,000;
- Halton Borough Council: £70,000;
- London Borough of Lewisham Council: £70,000;
- Devon County Council: £90,000;
- Plymouth City Council: £60,000;
- Leeds City Council: £95,000;
- Stoke-on-Trent City Council: £120,000;
- Scottish Borders Council: £250,000;
- Telford & Wrekin Council: £90,000;
- London Borough of Barnet: £70,000;
- Cheshire East Council: £80,000;
- Croydon Council: £100,000;
- Norfolk County Council: £80,000;
- Midlothian Council: £140,000;
- Powys County Council: £130,000;
- North Somerset Council: £60,000;
- Worcestershire County Council: £80,000;
- Surrey County Council: £120,000.

5 RESOURCE IMPLICATIONS

5.1 The cost of purchasing a 10" 16 gigabyte iPad 4 for Members would be around £16,000 dependent on the best price available when the purchase is made. This cost can be met from the provision in the IT Strategy Fund.

5.2 In terms of the solution for officers, the cost of the Ericom Blaze software, if accredited, would be approximately £7,500. This can be met from the IT Capital Programme allocation. The costs for equipment for Senior Management Team (£2,800) and Revenues and Benefits staff (£1,800) can also be met from this budget. If the Cabinet Office does not approve of our remote working solution for officers using a 'cryptocard', and the Ericom Blaze software is not accredited, then consideration would have to be given to supplying equipment; the cost of this could be found by re-prioritising existing work programmes.

5.3 In addition there are on-going support costs of approximately £4,400 per annum to be added to the Capita IT contract. This figure is based on the worst case scenario and includes support for 80 officer devices should this prove necessary. The figure would reduce if support was required for Member iPads and SMT and Revenues and Benefits staff equipment only.

6 LEGAL IMPLICATIONS

6.1 The Monitoring Officer has been consulted and advises that the requirements of Members set out in this report are consistent with the Council's Ethical Framework and Code of Conduct.

I confirm that the above recommendation does not depart from Council policy and that appropriate consideration has been given to any budgetary and legal implications.

SMT Lead Officer Signature: _____

Head of Information and Customer Services

Background Papers:-

None.

For further information please contact Sarah Fowler (Head of Information and Customer Services) on:-

Phone: 01702 546366
Email: sarah.fowler@rochford.gov.uk

If you would like this report in large print, Braille or another language please contact 01702 318111.

Corporate Information Security Policy

1. Introduction

Information resources are vital to Rochford District Council (RDC) in the delivery of services to residents, businesses and visitors. Their availability, integrity, security and confidentiality are essential to maintain service levels, legal compliance and the public image and public perception of RDC.

It is important that citizens are able to trust RDC to act appropriately when obtaining and holding information and when using the authority's facilities. It is also important that information owned by other organisations made available to RDC under secondary disclosure agreements is also treated appropriately by RDC.

Any Public Authority that uses or provides information resources has a responsibility to maintain, safeguard them, and comply with the laws governing the processing and use of information and communications technology.

The Executive and Chief Executive of RDC have ultimate responsibility and endorse the adoption and implementation of this Information Security policy. Delegated responsibilities are set out in section 6 and rest with the Senior Management Team and with the ICT and Web Manager with regard to the maintenance and review of the Corporate Information Security policy, Conditions of Acceptable Use and Personal Commitment Statements as well as local policies and procedures.

This policy is designed to provide an appropriate level of protection to the information for which RDC is responsible. Supporting this policy is a set of information security technical controls which form the minimum standard that a partner has to comply with. Individual organisations can strengthen these policies through local policies and procedures, but cannot weaken them.

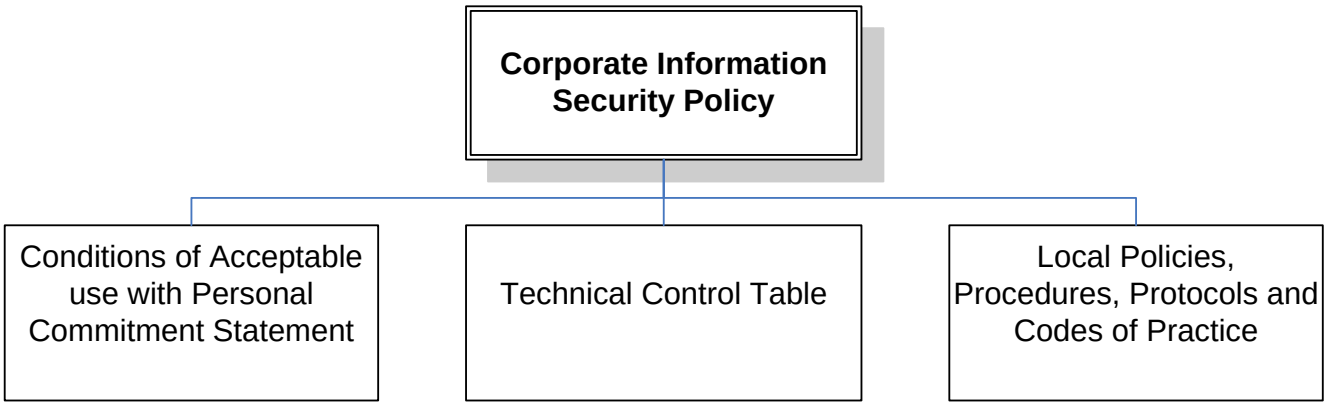
It is unacceptable for RDC information resources to be used to perform unethical or unlawful acts.

The key aspects of this policy and all associated policies have been developed in accordance with the British Standard for Information security BS7799 – 3:2006 which is harmonised with ISO/IEC 27001:2005.

This Corporate Information Security policy is supported by further policies, procedures, standards and guidelines. In addition to the RDC policy, users who are granted access to information owned by other organisations will be subject to the policy requirements of the information owners. Details of these policies will be provided before access is granted.

2.

Information Security Framework



3. Objectives

The objectives of the Corporate Information Security Policy are to ensure that:

- All users are aware of these policy statements and associated legal and regulatory requirements and of their responsibilities in relation to Information Security;
- All RDC property including equipment and information are appropriately protected;
- The availability, integrity and confidentiality of RDC information is maintained;
- A high level of awareness exists of the need to comply with Information Security measures;
- Unauthorised access to software and information is prevented;
- The risk of the misuse of e-mail services is reduced;
- The network and network resources are protected from unauthorised access;
- Guidance is provided on handling information of each classification in different circumstances and locations including creation, modification or processing, storage, communication, retention and deletion, disposal or destruction;
- Unwanted incidents such as virus infections, deliberate intrusion and attempted information theft are managed;
- Unauthorised access, damage and interference to business premises, Information and Information Technology is prevented.

4. Scope

The scope of this policy is for any employee, elected member, agency worker, third party organisation or other authorised personnel.

5. Legal and regulatory obligations

RDC will comply with all relevant legislation affecting the use of information and communication technology. All users must be made aware of and comply with current legislation as they may be held personally responsible for any breach.

A list of key legislation and regulations, with a brief description of each can be found in Appendix A.

6.

Roles and Responsibilities

Chief Executive

The Chief Executive is ultimately responsible for ensuring that all Information is appropriately protected.

Senior Management Team

This policy has been written by the Essex Online Partnership, and additional policies, procedures and standards have been written by the ICT and Web Manager. The Senior Management Team is responsible for the review and approval of the Corporate Information Security Policies and procedures, which are reviewed and re-issued each year. They are also responsible for approving and overseeing all information security related projects and initiatives. Rochford District Council **must** appoint a Senior Information Risk Owner (SIRO) to ensure there is accountability;

The SIRO **must** provide written judgement of the security and use of the business assets at least annually to support the audit process and provide advice to the accounting officer on the content of their statement of internal control.

Information Security Officer

This role is fulfilled by the ICT and Web Manager who is responsible for the day to day management of information security activities, and for responding to Information Security Incidents.

SIRO (Senior Information Risk Owner)

Local Government Association guidance and best practice suggests that the SIRO:

- Is the officer who is ultimately accountable for the assurance of information security at the Council;
- Champions information security at executive management team level;
- Owns the corporate information security policy;
- Provides an annual statement of the security of information assets (as part of the audit process);
- Receives strategic information risk management training at least once a year

The SIRO is not intended to be a new post but rather a newly-defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with IT, but takes a broader view of our information assets as a whole, in any form. This role is undertaken by the Head of Finance.

Risk Manager

The Risk Manager is responsible for the evaluation of the organisation's exposure to risk and controlling these exposures through such means as mitigation, avoidance, management or transference. This role is usually held by the **SIRO or ITSO (IT Security Officer)**.

Information Owners (also referred to as Information Asset Owners)

The role of the Information Asset Owner is to understand what information is held and in what form, how it is added to and/or removed, who has access, and why. They are tasked with ensuring that the best use is made of information, and receive and respond to requests for access.

They are responsible for:

- Assessing the risks to the information and data for which they are responsible in accordance with Rochford District Council Risk Management Methodology.; Defining the appropriate protection of their information taking into consideration the sensitivity and value of the information;
- Information owners will be responsible for defining the value of information, and identifying the risks associated with the information, so they must classify their information, and define the controls for its protection.

Heads of Service and Line Managers

Are responsible for:

- Ensuring that their employees are fully conversant with this Policy and all associated, Policies, Standards, Procedures, Guidelines and relevant legislation, and are aware of the consequences of non-compliance;
- Developing procedures, processes and practices which comply with this Policy for use in their business areas;
- Ensuring that all external agents and third parties defined in the scope of this Policy are aware of their requirement to comply;
- Ensuring that when requesting or authorising access for their staff, they comply with the standards and procedures defined by the Information Owners;
- Notifying the Information Security Officer of any suspected or actual breaches or perceived weaknesses of information security.

Employees

Are responsible for:

- Ensuring that they conduct their business in accordance with this Policy and all applicable supporting policies;
- Familiarising themselves with this Policy, and all applicable supporting Policies, Procedures, Standards and Guidelines.

Employees responsible for management of third parties must ensure that the third parties are contractually obliged to comply with this Policy.

Users of systems and information

Those who are granted access to Information and information systems must:

- Only access systems and information, including reports and paper documents to which they are authorised;
- Use systems and information only for the purposes for which they have been authorised;
- Comply with all applicable legislation and regulations;
- Comply with the controls defined by the Information Owner;
- Comply with all Rochford District Council Policies, Standards, Procedures and Guidelines, and the policies and requirements of other organisations when granted access to their information;
- Not disclose confidential or sensitive information to anyone without the permission of the Information Owner, and ensure that sensitive information is protected from view by unauthorised individuals;
- Keep their passwords secret, and not allow anyone else to use their account to gain access to any system or information;
- Notify the ICT and Web Manager of any actual or suspected breach of Information Security, or of any perceived weakness in the organisation's Security Policies, Procedures, Practices, Process or infrastructure in accordance with the Incident Reporting and Management Procedure;
- Protect Information from unauthorised access, disclosure, modification, destruction or interference;
- Not attempt to disable or bypass any security features which have been implemented;
- All users are responsible for reporting any actual or suspected Information Security incidents or problems and assisting with their resolution;
- The ICT and Web Manager is responsible for managing the resolution of each incident and its underlying problem.

7. Approach to Risk Management

Risk management is defined as co-ordinated activities to direct and control an organisation with regard to risk.

The RDC approach to information security is in accordance with the Public Services Network (PSN) Risk Management & Accreditation Reference Document as published by the Cabinet Office. (The PSN is a multi-supplier environment providing end-to-end service assurance for security, integrity and reliability, comprising a network of networks operating at a minimum Business Impact Level of IL2 for Confidentiality and Integrity). RDC uses the risk management process to focus on providing the business with an understanding of risks to allow effective decision-making to control risks. The risk management process is an on-going activity that aims to continuously improve the efficiency and effectiveness of information security.

RDC has a Corporate Risk Register that is reviewed on a regular basis. This includes a risk around information security. There are also Risk Registers at Divisional level that cover in more detail the risks relating to IT and information security

8. Incident Reporting and Management

Rochford District Council has established an Incident Reporting and Management framework which is in accordance with the PSN Incident and Problem Management Document as published by the Cabinet Office. That part of this policy is managed by the Head of Information and Customer Services and the ICT and Web Manager.

9. Review

The Essex OnLine Partnership **must** undertake an annual review of Information Security Policies and associated papers to ensure they still comply with current good practice and standards as well as an Equality Impact Assessment if policies change. It is the duty of Rochford District Council to review Information Security management arrangements in place and review local arrangements contained within local policies, including an annual IT health check carried out by a CHECK accredited independent expert. (CHECK is an accreditation framework provided by the Information Assurance (IA) arm of GCHQ, based in Cheltenham, Gloucestershire.)

10. Awareness, Compliance and Auditing

Rochford District Council will ensure compliance with the Information Security Policy through:

10.1 Awareness

a. Information Security will be included in the induction programme.
b. An ongoing Information Security awareness programme will be implemented for all users including third parties.
c. All users will receive appropriate awareness training and updates in organisational policies and procedures as relevant to their job functions.
d. All users will be required to sign a personal commitment statement.

10.2 Compliance

Compliance with this Policy is mandatory, and non-compliance with this Information Security Policy, supporting policies, procedures and standards may result in disciplinary action, or termination of contracts under which a business provides services.

10.3 Auditing

a. Carrying out Internal audits and where appropriate keeping audit logs in line with legislation and Rochford District Council document retention policy.

b. Where connectivity to other secure networks such as N3 or GSi is established, Rochford District Council **must** submit to (and fund) an audit of their security procedures and practices in the form of an annual IT Health check, and implement any recommendations to demonstrate that they meet the requirements of this security policy.

11. Monitoring

Where appropriate; monitoring arrangements are put in place to ensure compliance with policy objectives, guidelines and standards.

12. Documentation

Document Owners: Essex OnLine Partnership Management Group and Rochford District Council
Document Authors: Essex OnLine Partnership Resource Team and Rochford District Council

Disclaimer:
This printed version may not be the current version.
A current version may be obtained in the required format from the EOLP Resource Team or Rochford District Council Intranet.

Version History

Version	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
0.1	Oct 2007	EOLP	EOLP Resource Team		First draft
1.0	28th Mar 2008	EOLP	EOLP Resource Team	EOLP Information Security Working Group (ISWG)	Changes agreed by the EOLP Information Security working group on 17-03-08.
2.0	20th Feb 2009	EOLP	EOLP Resource Team	EOLP ISWG	Changes agreed by the EOLP Information Security working group on 05-02-2009.
2.1	30th June 2009	EOLP	EOLP Resource Team	EOLP ISWG	Equality Impact Assessment carried out changes to Section 9 Review to include EQIA and Section 12 Documentation to provide the policy in the required format
2.2	25th Jan 2010	EOLP	EOLP Resource Team		Combined all policies into the Corporate IS Policy and created a set of Technical Control in support of this policy.
2.3	112th Feb 2010	EOLP	EOLP Resource Team		Moved Definitions to Technical Control spreadsheet, minor changes following Information Security working group meeting.
3.0	1st March 2010	EOLP	EOLP Resource Team	EOLPMG	Removed the highlights that indicated the changes that were made.
3.1	23rd June 2011	EOLP	EOLP Resource Team		Incorporated PSN CoCo requirements
4.0	14th July	EOLP	EOLP Resource	EOLP ISWG	Incorporated feedback from

Corporate Information Security Policy

Version	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
	2011		Team		ISWG
5.0	27th Sept 2011	EOLP	EOLP Resource Team	EOLP ISWG	Additional text for Information Owners and added role of Risk Manager, text taken from PSS IA glossary. Changes to Approach to Risk and Incident Management
5.1	18th Oct 2012	EOLP	EOLP Resource Team	EOLP ISWG	Risk Manager section changed DSO to SIRO
6.0	Nov 2012	EOLP	EOLP Resource Team	EOLP ISWG	Version 6 Issued
6.1	17 July 2013	The Executive	ICT and Web Manager	Head of Information and Customer Services	Localised to RDC

-

Appendix A

This is a list of key legislations and regulations.

Data Protection Act 1998 and EU Directive on Data Protection

Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it.
Unauthorised disclosure of Council or client personal information is prohibited and could constitute a breach of this Act.
Further in formation on this Act can be obtained from the Data Protection Officer *<name, contact>*

Computer Misuse Act 1990

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is not allowed and would constitute an offence under this Act for which the penalties are imprisonment and/or a fine.

This Act addresses the following offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

Copyright, Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.

Companies Act 1985

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.

Freedom of Information Act 2000

Gives a general right of access to all types of data and information that has been recorded by the Council. There are exemptions to the right of access, but the Council must assist applications for information and proactively make details available about the Council. The Council must know what records it holds, where they are stored and must avoid them being lost.

Conditions of Acceptable Use and Personal Commitment Statement

1 Introduction

The Conditions of Acceptable Use document defines acceptable use of Information and Communication Technology within Rochford District Council (RDC) and is in support of the Corporate Information Security Policy.

2 Definitions

Information security is the preservation of:

- **Confidentiality**: ensuring that information is accessible only to those authorised to have access;
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods;
- **Availability**: ensuring that authorised users have access to information and associated assets when required.

The Conditions of Acceptable Use and other Information Security policies are underpinned by the Personal Commitment Statement which details a list of specific compliance requirements.

3 Scope

This applies to any employee, elected member, agency worker, third party organisation or other authorised personnel

4 Authority

This policy is supported by the Executive and Senior Management Team of RDC.

5 Objectives

The objective of the Acceptable Use Policy is:

- To protect information and communication technology from unacceptable use.

6 Roles and responsibilities

All roles and responsibilities are outlined in the Corporate Information Security Policy.

7 Conditions of Acceptable Use

You **must not:**

- Access or attempt to access any computer material, (that is a program or data), that you are not authorised to access;
- Access or attempt to access a computer system with the intent to commit or facilitate the commission of a criminal offence;
- Use a colleague's credentials to access the Public Services Network (PSN) (The PSN is a multi-supplier environment providing end-to-end service assurance for security, integrity and reliability, comprising a network of networks operating at a minimum Business Impact Level of IL2 for Confidentiality and Integrity) and will equally ensure that your credentials are not shared and are protected against misuse;
- Attempt to access the PSN other than from IT systems and locations which you have been explicitly authorised to use for this purpose;
- Transmit information via the PSN that you know, suspect or have been advised is of a higher level of sensitivity than your PSN domain is designed to carry;
- Transmit information via the PSN that you know or suspect to be unacceptable within the context and purpose for which it is being communicated;

- Make false claims or denials relating to your use of the PSN (e.g. falsely denying that an e-mail had been sent or received);
- Carry out unauthorised modifications to any computer material;
- Undertake any unlawful, libellous, immoral or offensive activities, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to material of a pornographic, sexual, violent or criminal content, racist, sexist or otherwise discriminatory nature;
- Install software without the approval of the ICT and Web Manager *a*nd this **must** be for business purposes subject to compliance with license restrictions;
- Send information marked PROTECTED or above over public networks such as the Internet unless approved encryption has been applied to it;
- Send or forward any chain emails (e.g. jokes) except to report them as defined in the Security Incident Reporting and Management Procedures;
- Use RDC's facilities or RDC identity for commercial purposes outside of the authority or remit of RDC or for personal financial gain unless authorised to do so;
- Rely on building controls such as security doors to prevent unauthorised access or use;
- Do anything that would compromise the security of the information as defined in Corporate Information Security Policy;
- Attempt to introduce viruses, Trojan horses or any other malware into the system, and must not attempt to disable or bypass anti-virus protection or delay updates provided on your computer;
- Disclose in writing, speech or electronically information held by RDC unless you are authorised to do so and recipients are authorised to receive it;
- Attempt to disable measures which prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation);
- Attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;
- Remove equipment or information from your employer's premises without appropriate approval;
- Disable anti-virus protection provided at your computer;
- Store data on a local workstation unless there is an approved business case and backup capability;
- Install any third party screensaver or wallpapers;
- Move any ICT equipment. The procedure for moving ICT equipment must be followed;
- Connect anything to any RDC ICT system without following and complying with the Procedure for using portable electronic devices and linking them to the RDC ICT System;

You **must:**

- Lock equipment or log out of the workstation when leaving it unattended even for a short time;
- Are responsible for helping to maintain the security of information held by RDC;
- Protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, you will not write down or share your password other than for the purposes of placing a secured copy in a secure location at your employer's premises);
- Seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts

immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;
- Take appropriate steps to secure the equipment and information to which you have access when your equipment or information is unattended;
- Report actual or suspected information security incidents, events or weaknesses to the ICT and Web Manager;
- Report any detected viruses to the Capita SIS Helpdesk immediately and **ONLY** to the Capita SIS Helpdesk*;*
- When printers, photocopiers or faxes are used for protected, restricted or sensitive information they must be attended by an appropriate person if the printer doesn't support printer mailboxes (such as private or locked print);
- Security of electronic information is achieved through the use of logins and passwords. You must log in using your own login name and a secure password known only to you;
- Report all faults to the Capita SIS Helpdesk;
- You are provided with facilities for business use only; limited personal use is acceptable if it meets the criteria defined in other policies;
- If you are a manager, you must also ensure that users you are responsible for are aware of, and comply with, this policy;
- If you are a user of N3, you must also comply with the NHS Statement of Compliance requirements;
- If you are a user of N3, you must also comply with the NHS Statement of Compliance for 3rd Parties;
- If you access any systems such as NHS or Government, through other secure networks such as EssExtranet you must only use those systems for the purpose for which they have been authorised, and they must not establish, or attempt to establish an onward connection once they have gained access to the end system;
- Make yourself aware of RDC's security policies and procedures together with any additional requirements which may be associated with connection to secure networks such as PSN;
- Protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by you via the PSN to the same level as you would paper copies of similar material;
- Use the provided facilities economically;
- Take precautions to protect all computer media and portable computers when carrying them outside your organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);
- Comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that RDC informs you are relevant;
- Inform your manager prior to your departure from employment of any important information held in your account;
- Ensure that data that has been authorised to be stored on a local workstation is backed up regularly.

Conditions of Acceptable Use and Personal Commitment Statement

Acceptable Use of email

You **must not:**

- Use e-mail for offensive or unlawful activities, commercial purposes or personal financial gain;
- Access or disclose other people's e-mail without their permission.
- Subscribe to services using RDCs e-mail address unless representing RDC;
- Send unsolicited, irrelevant or inappropriate e-mail to multiple newsgroups or mailing lists;
- Forward or disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;
  Use your GCSX email address as a sender field when emailing content from the Internet to GCSX ;
- Not knowingly disrupt RDC's e-mail service or send emails from another users address unless the email identifies the sender i.e. 'on behalf of';
- Auto-forward email from your RDC email account to any non-PSN email account.

You **must:**

- Always check that the recipients of e-mail messages are correct especially when using auto completion of email addresses so that potentially sensitive or protectively marked information is not accidentally released into the public domain;
- Disclose information received via the PSN only on a "need to know" basis;
- Protect the confidentiality of e-mail you view inadvertently;
- Follow RDC procedures for authorisation and notification if accessing someone else's e-mail;
- Comply with RDC policies and any UK law that applies to e-mail;
- Use personal and professional courtesy and consideration when using e-mail;
- Add security labels to each email that carries a protective marking of PROTECT or higher.

You **should not:**

- Rely exclusively on e-mail to archive or retain records;
- Access personal e-mail accounts directly or via the web;
- Send encrypted files via email unless implementing a business requirement such as protecting personal sensitive information.

You **should:**

- Make appropriate arrangements to make your e-mail available to ensure service continuity during any absence;
- Check with the sender if not sure about the authenticity of a message;
- Regularly check your e-mail inbox for new messages;
- Take care when you use the Reply to All function as this may be inappropriate.

Conditions of Acceptable Use and Personal Commitment Statement

Acceptable Use of the internet

You **must not:**

- Visit web sites that contain inappropriate material. These include but are not limited to pornography, extremist or racist organisations, dating web sites and chat rooms;
- Join forums or other forms of electronic notice board in the name of RDC other than for legitimate RDC use. Where passwords are required for forums or any other web or e-mail access outside RDC, different passwords should be used to those used for internal access;
- Publish a web site or anything on a web site that could bring RDC into disrepute;
- Use any sort of instant messaging software or peer-to-peer software for personal or professional reasons without prior consent from the ICT and Web Manager at RDC;
- Download software without prior consent from the ICT and Web Manager at RDC. Software includes but is not limited to screensavers, device drivers, shareware, browser add-ins, software patches, add-ons and updates. All software installations must comply with license agreements;
- Commit RDC to any agreements with third parties over the Internet without prior consent from the appropriate manager;
- Knowingly interfere with other people's use of the internet;
- Unreasonably offend any colleague, or promote/engage in discriminatory behaviour in the workplace.

You **must:**

- Use personal and professional courtesy and consideration when using the internet.

Acceptable Use of Removable Media

You **must:**

- Use removable media in accordance with the Corporate Information Security Policy and Section 8 of this policy.

Acceptable Use of Authentication

You **must not**:

- Attempt to bypass or disable any security controls;
- Disclose your password to anyone other than for the purposes of placing a secured copy in a secure location at RDC's premises. You are accountable for any action taken using your login and password. If you are asked to log into a computer and allow support staff to access the network, you should note the date and time in case of later query;
- Ask anyone else for their password;
- Tell the system to store passwords so that it can access them without typing them in. Information security relies on the proper use of passwords;

You **must:**

- Maintain a network password which has to be a minimum of 8 characters long and must be a combination of characters and numbers with at least one character as a capital letter;
- If you find it necessary to record a password, for your own benefit, best efforts must be taken ensure that it is not accessible to anyone else.

You **should:**

- Change Passwords when a breach of security occurs or is suspected. If you suspect that your password is no longer secure, it must be changed immediately and follow the incident reporting procedure if appropriate.

Acceptable Use of your own device

You **must:**

- accept all terms and conditions in the Bring Your Own Device (BYOD) Policy and Commitment Statement to be allowed access to RDC services;
- Sign the BYOD Policy and Commitment Statement;
- Only use your own device if authorised by the ICT and Web Manager and your line manager in accordance with the BYOD Policy.

8 RDC specific

Personal Use of RDC systems including email and accessing the Internet via the network, Wi-Fi Connections, public access terminals or your own device

Limited personal use of RDC ICT facilities is acceptable subject to the following factors being complied with:

Personal use **must not:**

- Interfere with the performance of your duties;
- Make use of information available to you that is not available to the public;
- Result in any additional cost to RDC;
- Reflect adversely on the reputation of the RDC;

Personal use **must:**

- Be in accordance with the Corporate Information Security Policy, standards and procedures. If personal use is abused, facilities may be withdrawn;
- Be in your own time (i.e. before or after work, or during your lunch break);

You **must not:**

- Under any circumstances use personal credit/debit cards over the Internet, bid on online auctions or use online banking for personal usage from RDC computer equipment;
- Let personal use of e-mail interfere with your employment or other obligations to RDC;
- Download any files for personal use onto your PC / terminal, RDC's servers, CDs, DVDs USB sticks, memory cards or other removable media or device;
- Download any attachments from web mail sites, social media sites or any other web site as they pose a virus threat;
- Use RDC's facilities for product/service advertisement, commercial activities or political lobbying;
- Use RDC's facilities or RDC identity for commercial purposes outside of the authority or remit of RDC or for personal financial gain unless authorised to do so;
- Use RDC's email addresses to receive receipts for goods or services bought online for non-RDC use;

- Subscribe to non-business related web sites that send automated emails to a RDC e-mail address;
- Access personal e-mail accounts directly. Access via the web is permitted.

You **must:**
- Only use the internet for personal purposes in your own time (i.e. before or after work, or during your lunch break);
- Delete any personal emails received by your RDC email account(s) that contain a non work related attachment. Under no circumstances should you reply to it, forward it to other users or print it;
- Only use any Internet Connection provided by RDC in accordance with the Personal Use of RDC systems section of this Policy.

You **should:**
- Use the Staff Notice board on the Intranet to advertise Goods and Services. RDC reserves the right to withdraw any such service without reason.

You **may:**
- Use the Internet for personal transactions that do not involve RDC's ICT System in any way other than to access the Internet.

You **acknowledge that:**
- RDC reserves the right to limit or remove access to non-business related web sites without prior notice, if the ICT System is being overloaded or otherwise adversely affected by Internet use;
- All emails to and from the Rochford.gov.uk email address are automatically stored in the email archiver for a period of 3 years and can be retrieved if necessary. RDC uses software to alert it to e-mail attachments that may be unsuitable. This monitors internal, incoming and outgoing e-mails. Capita SIS will know the content of personal messages that have attachments identified by this software. The employee's Head of Service may be alerted to these e-mails;
- As with all matters of conduct whilst at work, employees' line managers have a responsibility for supervising the use of email and Internet facilities, particularly as the unregulated nature of the Internet has the potential for wasting employees' time and can be open to abuse. Heads of Service can ask for a record of an employee's use of the internet and email where there is concern about activity. The use of the Internet is monitored on a 24/7 basis and the ICT Client side receive monthly reports of the top internet users amongst staff. These reports may be used to investigate internet activity if it appears to be of an unusual nature.

Conditions of Acceptable Use and Personal Commitment Statement

Acceptable Use of Removable Media

You **must:**

- Use removable media in accordance with the Corporate Information Security Policy.

Mobile Technology

You **must:**

- Comply with the Procedures for using RDC ICT equipment outside of the work place.

You **must not:**

- Access mobile services from outside the UK unless you have been made aware of the risks of using mobile technology abroad by reading the Procedure for using Mobile Technology abroad;

Accessing RDC systems remotely

You **must not:**

- Access RDC systems remotely unless you are authorised to do so by the ICT and Web Manager.

You **must:**

- Only access RDC systems remotely using hardware and/or software provided to you by RDC for that purpose;
- When using your own equipment to access RDC systems remotely only do in in accordance with the RDC Corporate Information Security Polices and Procedures.

9 Personal Commitment Statement

Introduction

This personal commitment statement is in support of RDC Corporate Information Security Policy.

Scope

A personal commitment statement **must** be in place for every user of RDC information and resources.

"I

- *acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes;*
- *agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address;*
- *will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;*
- *will protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises);*

- *will not attempt to access any computer system that I have not been given explicit permission to access;*
- *will not attempt to access the PSN other than from IT systems and locations which I have been explicitly authorised to use for this purpose*
- *will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry;*
- *will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;*
- *will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);*
- *will protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;*
- *will not send information marked PROTECTED or above over public networks such as the Internet unless approved encryption has been applied to it;*
- *will check that the recipients of e-mail messages are correct especially when using auto completion of email addresses so that potentially sensitive or protectively marked information is not accidentally released into the public domain;*
- *will not auto-forward email from my PSN account to any non-PSN email account;*
- *will disclose information received via the PSN only on a "need to know" basis;*
- *will not forward or disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;*
- *will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;*
- *will securely store or destroy any printed material in accordance with the RDC Documentation Retention Policy;*
- *will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN (this might be by closing the e-mail program, logging-off from the computer, activating a password-protected screensaver, etc., so as to require a user logon for activation); and*
- *will not leave information unattended in such a state as to risk unauthorised disclosure of information;*
- *where my organisation has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection;*
- *will make myself familiar with the security policies, procedures and any special instructions that relate to the PSN;*
- *will inform the ICT and Web Manager immediately if I detect, suspect or witness an information security incident or problem that may be a breach of security;*
- *will not knowingly attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;*

Conditions of Acceptable Use and Personal Commitment Statement

- *will not remove equipment or information from my employer's premises without appropriate approval;*
- *will take precautions to protect all information and computer media and portable computers when carrying them outside my organisations' premises (e.g. not leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);*
- *will not knowingly introduce viruses, Trojan horses or other malware into the system or PSN;*
- *will not disable anti-virus protection or delay updates provided at my computer;*
- *will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and*
- *if I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account."*

I am aware of the disciplinary procedures of RDC in the event of non-compliance with this commitment

When I use my own device;
"I

- *accept all terms and conditions in the Bring Your Own Device(BYOD) Policy and Commitment Statement to be allowed access to RDC services;*
- *will sign the BYOD Policy and Commitment Statement.*

Signature…….Date……

Please print

Name	
Job Title	
Place of Work	

10. Documentation

Document Owners: Essex OnLine Partnership Management Group and Rochford District Council
Document Authors: Essex OnLine Partnership Resource Team and Rochford District Council

Disclaimer

This may not be the current version. RDC's Intranet will contain the current version of this procedure and you are advised to check that you referring to that version. If you need this information in large print, Braille or another language please contact the ICT and Web Team.

Version History

Version No	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
0.1	October 2007	EOLP	EOLP (RT)		First draft

Conditions of Acceptable Use and Personal Commitment Statement

Version No	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
0.2	October 2007	EOLP IS working group	EOLP (RT)		Agreed by the EOLP Information Security working group on 10-10-07
0.3	November 2007	EOLP	EOLP (RT)		Changed numbering following comments from Rochford
0.4	November 2007	EOLP	EOLP (RT)		Amended based on group feedback.
0.5	December 2007	EOLP	EOLP (RT)		Added third definition
0.6	January 2008	EOLP	EOLP (RT)		Policy statement changes to ensure the language used is in line with the appropriate legal terms.
0.7	March 2008	EOLP	EOLP (RT)		Incorporated recommendations from Information Security consultants Hytec
0.8	March 2008	EOLP	EOLP (RT)	EOLP (ISWG)	Changes agreed or adjusted following Hytec recommendations by the EOLP Information Security working group on 10-03-08
1.0	28 March 2008	EOLP	EOLP (RT)	EOLP (ISWG)	Changes agreed by the EOLP Information Security working group on 17-03-08.
2.0	20 February 2009	EOLP	EOLP (RT)	EOLP (ISWG)	Changes agreed by the EOLP Information Security working group on 05-02-2009.
2.1	30 June 2009	EOLP	EOLP (RT)	EOLP (ISWG)	Equality Impact Assessment carried out change to Section 9 Documentation to provide the policy in the required format
2.2	25 January 2010	EOLP	EOLP (RT)		Updated with statements following publication of GCSx Code of Connection V4.1
2.3	12 February 2010	EOLP	EOLP (RT)	EOLP (ISWG)	Change of name, inclusion of Personal Commitment Statement and changes identified in the ISWG meeting
3.0	1March 2010	EOLP	EOLP (RT)	EOLPMG	Removed the highlights that indicated the changes that were made.
3.1	23 June 2011	EOLP	EOLP (RT)		Incorporated PSN CoCo requirements
4.0	14 July 2011	EOLP	EOLP (RT)	EOLP (ISWG)	Incorporated feedback from ISWG
5.0	July 2012	EOLP	EOLP (RT)	EOLP (ISWG)	Added additional statements to sections 7 and 9 to comply with the PSN CoCo
5.1	Sept 2012	EOLP	EOLP (RT)	EOLP (ISWG)	Added Bring Your Own Device statements
5.2	Oct 2012	EOLP	EOLP (RT)	EOLP (ISWG)	Updated following feedback on BYOD
5.3	Oct 2012	EOLP	EOLP (RT)	EOLP (ISWG)	Updated PSN statements to reflect PSN CoCo V2.7 issued Aug 2012 merged GCSX section with general as this now applies to all staff under the PSN
6.0	Nov 2012	EOLP	EOLP (RT)	EOLP (ISWG)	Minor changes following consultation
6.1	17 July 2013	RDC	RDC (ICTWM)	RDC (HICS)	Localised to RDC