Policy Document

Information Security Policy Overview

[23/08/2011]

Document Control

Organisation	Redditch Borough Council
Title	Information Security Policy Overview
Author	Mark Hanwell
Filename	Information Security Policy Overview.doc
Owner	Mark Hanwell – ICT Transformation Manager
Subject	Information Security Policy Overview
Protective Marking	Unclassified
Review date	23/08/2011

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Head of Business Transformation	Deborah Poole	23rd August 2011

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1 Introduction

In order to ensure the continued delivery of services to our customers, Redditch Borough Council is making ever increasing use of Information and Communication Technology (ICT) and customer information held by the Council and other public sector organisations.

The information that the Council holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

In order to build public confidence and ensure that the Council complies with relevant statutory legislation, it is vital that Redditch Borough Council maintains the highest standards of information security. As such, a number of policies are in place to maintain these high standards of information security.

2 Purpose

This document provides a summary of the Information Security Policies developed by Redditch Borough Council. The objective of these policies is to ensure the highest standards of information security are maintained across the Council at all times so that:

- The public and all users of the Council's information systems are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- All legislative and regulatory requirements are met.
- The Council's ICT equipment and facilities are used responsibly, securely and with integrity at all times.

The policies developed by Redditch Borough Council are based on industry good practice and intend to satisfy the requirements set out by the Government Connect Secure Extranet Code of Connection (CoCo). The policies include:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- IT Access Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Human Resources Information Security Standards.
- Information Protection Policy.
- Computer, Telephone and Desk Use Policy.
- Legal Responsibilities Policy.
- Remote Working Policy.
- Removable Media Policy.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.
- IT Infrastructure Policy.

Each policy follows the same format and includes:

- Policy Statement.
- Scope – who the policy applies to.
- Risks – the risks the policy aims to mitigate.
- Applying the Policy.

- Key Messages.

3 Information Security Policy Documents

3.1 Email Policy

Policy Statement

Redditch Borough Council will ensure all users of Council email facilities are aware of the acceptable use of such facilities.

Key Messages

- All emails that are used to conduct or support official Redditch Borough Council business must be sent using a "@Bromsgroveandredditch.gov.uk" address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@RedditchBc.gcsx.gov.uk".
- Non-work email accounts **must not** be used to conduct or support official Redditch Borough Council business.
- Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email.
- All official external e-mail must carry the official Council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council's Equal Opportunities policy.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT and RESTRICTED material.
- Automatic forwarding of email must be considered carefully to prevent PROTECT and RESTRICTED material being forwarded inappropriately.

3.2 Internet Acceptable Usage Policy

Policy Statement

Redditch Borough Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities.

Key Messages

- Users must familiarise themselves with the detail, essence and spirit of this policy before using the Internet facility provided.
- At the discretion of your line manager, and provided it does not interfere with your work, the Council permits certain personal use of the Internet in your own time (for example during your lunch-break).
- Users are responsible for ensuring the security of their Internet account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.
- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

3.3 Software Policy

Policy Statement

Redditch Borough Council will ensure the acceptable use of software by all users of the Council's computer equipment or Information Systems.

Key Messages

- All software acquired must be purchased through the ICT Department
- Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
- Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.
- Unauthorised changes to software **must not** be made.
- Users are not permitted to bring software from home (or any other external source) and load it onto Council computers.
- Users **must not** attempt to disable or reconfigure the Personal Firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

3.4 IT Access Policy

Policy Statement

Redditch Borough Council will establish specific requirements for protecting information and information systems against unauthorised access.

Redditch Borough Council will effectively communicate the need for information and information system access control.

Key Messages

- All users must use **strong** passwords.
- Passwords must be protected at all times and must be changed at least every 42 days.
- User access rights must be reviewed at regular intervals.
- It is a user's responsibility to prevent their userID and password being used to gain unauthorised access to Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the ICT department.
- Partners or 3rd party suppliers must contact the ICT Helpdesk before connecting to the Redditch Borough Council network.

3.5 GCSx Acceptable Usage Policy and Personal Commitment Statement

Policy Statement

It is Redditch Borough Council policy that all users of GCSx understand and comply with corporate commitments and information security measures associated with GCSx.

Key Messages

- Each GCSx user must read, understand and sign to verify they have read and accepted the policy.

3.6 Human Resources Information Security Standards

Policy Statement

Redditch Borough Council will ensure that individuals are checked to ensure that they are authorised to access Council information systems.

Redditch Borough Council will ensure that users are trained to use information systems securely.

Redditch Borough Council will ensure that user access to information systems is removed promptly when the requirement for access ends.

Key Messages

- Every user must be aware of, and understand, the following policies :
    - Information Protection Policy .
    - Email Policy
    - Internet Acceptable Usage Policy.
    - Software Policy .
    - GCSx Acceptable Usage Policy and Personal Commitment Statement.
    - IT Access Policy.
    - Information Security Incident Management Policy

- Background verification checks must be carried out on all users.
- Users who require access to PROTECT and RESTRICTED information and / or require use of the Government Connect Secure Extranet (GCSx) email facility **must** be cleared to "Baseline Personnel Security Standard".
- All users must receive appropriate information security awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role.
- Processes must be implemented to ensure that all access rights of users of Council information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

3.7 Information Protection Policy

Policy Statement

Redditch Borough Council will ensure the protection of all information assets within the custody of the Council.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Key Messages

- The Council must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF).

- Information up to RESTRICTED sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until they understand and agree the legislated responsibilities for the information that they will be handling.
- PROTECT and RESTRICTED information **must not** be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing PROTECT or RESTRICTED classified information to any external organisation is also **prohibited**, unless via the GCSx email.
- Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating PROTECT or RESTRICTED material.
- The disclosure of PROTECT or RESTRICTED classified information in any way other than via GCSx email is a disciplinary offence.

3.8 Computer, Telephone and Desk Use Policy

Policy Statement

Redditch Borough Council will ensure that every user is aware of, and understands, the acceptable use of Redditch Borough Council's computer and telephony resources and the need to operate within a "clear desk" environment.

Key Messages

- Users must adhere to Redditch Borough Council Telephone Acceptable Use Policy / Code of Practice at all times.
- Users must maintain a clear desk at all times.
- Redditch Borough Council PROTECT or RESTRICTED information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

3.9 Legal Responsibilities Policy

Policy Statement

Redditch Borough Council will ensure that every user is aware of, and understands, their responsibilities under the Data Protection Act 1998 and other relevant legislation.

Key Messages

- The Council will ensure compliance with the Data Protection Act 1998.
- The Council has established a number of roles to assure compliance of this policy.
- Every Council user has a duty to provide advice and assistance to anyone requesting information under the Freedom of Information Act.
- All Councillors must accept responsibility for maintaining Information Security standards within the Council.

3.10 Remote Working Policy

Policy Statement

Redditch Borough Council provides users with the facilities and opportunities to work remotely as appropriate. Redditch Borough Council will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities.

Key Messages

- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices and not emailing PROTECT or RESTRICTED information to a non-Council email address.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- It is the user's responsibility to ensure that access to all PROTECT or RESTRICTED information is controlled – e.g. through password controls.
- All PROTECT or RESTRICTED data held on portable computer devices must be encrypted.

3.11 Removable Media Policy

Policy Statement

Redditch Borough Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

Key Messages

- It is Redditch Borough Council policy to prohibit the use of all removable media devices. The use of removable media devices will only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by IT **must not** be used.
- All data stored on removable media devices **must** be encrypted where possible.
- Damaged or faulty removable media devices must not be used.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.

3.12 Information Security Incident Management Policy and Procedure

Policy Statement

Redditch Borough Council will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the Council.

Key Messages

- All staff should report any incidents or suspected incidents immediately by contacting ICT.
- We can maintain your anonymity when reporting an incident if you wish.

3.13 Communications and Operation Management Policy

Policy Statement

Redditch Borough Council will ensure the protection of the Council IT service (including any information systems and information processing equipment used by the Council) against malware and malicious and mobile code.

Only authorised changes will be made to the Council IT service (including any information systems and information processing equipment).

Information leakage will be prevented by secure controls.

Key Messages

- Changes to the Council's operating systems must follow the Council's formal change control procedure.
- Unpatchable software must not be used where there is GCSx connection provided.
- Appropriate access controls shall be put in place to prevent user installation of software and to protect against malicious and mobile code.
- Regular backups of essential business information will be taken to ensure that the Council can recover from a disaster, media failure or error.
- Storage media must be handled, protected and disposed of with care.
- Audit logs for RESTRICTED data and GCSx services must be kept for a minimum of six months.
- Connections to the Council network are made in a controlled manner.
- An annual health check must be made of all Council IT infrastructure systems.

3.14 IT Infrastructure Security Policy

Policy Statement

There shall be no unauthorised access to either physical or electronic information within the custody of the Council.

Protection shall be afforded to:

- Sensitive paper records.
- IT equipment used to access electronic data.
- IT equipment used to access the Council network.

Key Messages

- PROTECT or RESTRICTED information, and equipment used to store and process this information, must be **stored** securely.
- Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by ICT, as appropriate. Keys are not stored near these secure areas or lockable cabinets.
- All general computer equipment must be located in suitable physical locations.
- Desktop PCs should not have data stored on the local hard drive.
- Non-electronic information must be assigned an owner and a classification. PROTECT or RESTRICTED information must have appropriate information security controls in place to protect it.
- Staff should be aware of their responsibilities in regard to the Data Protection Act.

- Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.

4 Policy Compliance

If any user is found to have breached this policy, they may be subject to Redditch Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or ICT.

5 Policy Governance

The following table identifies who within Redditch Borough Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Transformation Manager
Accountable	Head of Business Transformation
Consulted	Corporate Management Team
Informed	All Council Employees, All Temporary Staff, All Contractors etc

6 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the ICT Transformation Manager.