Public Document Pack

# Appendices – Item 5

# Executive

Committee

Tue 13 Sep
2011
7.00 pm

Council Chamber
Town Hall
Redditch

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Access to Information - Your Rights

The Local Government (Access to Information) Act 1985 widened the rights of press and public to attend Local Authority meetings and to see certain documents. Recently the Freedom of Information Act 2000, has further broadened these rights, and limited exemptions under the 1985 Act.

Your main rights are set out below:-

- Automatic right to attend all Council and Committee meetings unless the business would disclose confidential or "exempt" information.
- Automatic right to inspect agenda and public reports at least five days before the date of the meeting.
- Automatic right to inspect minutes of the Council and its Committees (or summaries of business undertaken in private) for up to six years following a meeting.
- Automatic right to inspect lists of background papers used in the preparation of public reports.
- Access, upon request, to the background papers on which reports are based for a period of up to four years from the date of the meeting.
- Access to a public register stating the names and addresses and electoral areas of all Councillors with details of the membership of all Committees etc.
- A reasonable number of copies of agenda and reports relating to items to be considered in public must be made available to the public attending meetings of the Council and its Committees etc.
- Access to a list specifying those powers which the Council has delegated to its Officers indicating also the titles of the Officers concerned.
- Access to a summary of the rights of the public to attend meetings of the Council and its Committees etc. and to inspect and copy documents.
- In addition, the public now has a right to be present when the Council determines "Key Decisions" unless the business would disclose confidential or "exempt" information.
- Unless otherwise stated, all items of business before the Executive Committee are Key Decisions.
- (Copies of Agenda Lists are published in advance of the meetings on the Council's Website: **www.redditchbc.gov.uk**

**If you have any queries on this Agenda or any of the decisions taken or wish to exercise any of the above rights of access to information, please contact**
**Denise Sunman**
**Committee Support Services**

**Town Hall, Walter Stranz Square, Redditch, B98 8AH**
**Tel: (01527) 64252 ext 3270 Fax: (01527) 65216**
**e.mail: denise.sunman@bromsgroveandredditch.gov.uk Minicom: 595528**

# **Welcome** to today's meeting.

# Guidance for the Public

### *Agenda Papers*

The **Agenda List** at the front of the Agenda summarises the issues to be discussed and is followed by the Officers' full supporting **Reports**.

### *Chair*

The Chair is responsible for the proper conduct of the meeting. Generally to one side of the Chair is the Committee Support Officer who gives advice on the proper conduct of the meeting and ensures that the debate and the decisions are properly recorded. On the Chair's other side are the relevant Council Officers. The Councillors ("Members") of the Committee occupy the remaining seats around the table.

### *Running Order*

Items will normally be taken in the order printed but, in particular circumstances, the Chair may agree to vary the order.

***Refreshments :*** tea, coffee and water are normally available at meetings - please serve yourself.

### *Decisions*

Decisions at the meeting will be taken by the **Councillors** who are the democratically elected representatives. They are advised by **Officers** who are paid professionals and do not have a vote.

### *Members of the Public*

Members of the public may, by prior arrangement, speak at meetings of the Council or its Committees. Specific procedures exist for Appeals Hearings or for meetings involving Licence or Planning Applications. For further information on this point, please speak to the Committee Support Officer.

### *Special Arrangements*

If you have any particular needs, please contact the Committee Support Officer.

Infra-red devices for the hearing impaired are available on request at the meeting. Other facilities may require prior arrangement.

### *Further Information*

If you require any further information, please contact the Committee Support Officer (see foot of page opposite).

## *Fire/ Emergency instructions*

**If the alarm is sounded, please leave the building by the nearest available exit – these are clearly indicated within all the Committee Rooms.**

**If you discover a fire, inform a member of staff or operate the nearest alarm call point (wall mounted red rectangular box). In the event of the fire alarm sounding, leave the building immediately following the fire exit signs. Officers have been appointed with responsibility to ensure that all visitors are escorted from the building.**

**Do Not stop to collect personal belongings.**

**Do Not use lifts.**

**Do Not re-enter the building until told to do so.**

**The emergency Assembly Area is on Walter Stranz Square.**

# Declaration of Interests:
# Guidance for Councillors

DO I HAVE A "PERSONAL INTEREST" ?

- Where the item relates or is likely to affect your **registered interests** (what you have declared on the formal Register of Interests)

**OR**

- Where a decision in relation to the item might reasonably be regarded as affecting **your own** well-being or financial position, or that of your **family**, or your **close associates** more than most other people affected by the issue,

you have a personal interest.

WHAT MUST I DO? **Declare the existence, and nature, of your interest and stay**

- The declaration must relate to specific business being decided - a general scattergun approach is not needed

- **Exception** - where interest arises only because of your membership of another **public body**, there is no need to declare unless you **speak** on the matter.

- You **can vote** on the matter.

IS IT A "PREJUDICIAL INTEREST" ?

In general only if:-

- It is a personal interest ***and***

- The item affects your **financial position** (or conveys other benefits), or the position of your **family, close associates** or bodies through which you have a **registered interest** (or relates to the exercise of **regulatory functions** in relation to these groups)

  **and**

- A member of public, with knowledge of the relevant facts, would reasonably believe the interest was likely to **prejudice** your judgement of the public interest.

WHAT MUST I DO? **Declare and Withdraw**

BUT you may make representations to the meeting before withdrawing, **if** the public have similar rights (such as the right to speak at Planning Committee).

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Executive

Committee

**13th September 2011**

**7.00 pm**

**Committee Room 2 Town Hall**

## Agenda

**Membership:**

Cllrs:

Carole Gandy (Chair)
Michael Braley (Vice-Chair)
Juliet Brunner
Greg Chance
Brandon Clayton
Malcolm Hall
Jinny Pearce
Debbie Taylor
Derek Taylor

| | |
|---|---|
| **5.** **ICT Policies**<br>(Pages 113 - 260)<br>Head of Business Transformation | To seek approval for a number of ICT Policies provided by Central Government.<br>(Appendices attached)<br>**(No Direct Ward Relevance);** |

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# Policy Document

# Communications and Operation Management Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Communications and Operation Management Policy |
| **Author** | Mark Hanwell |
| **Filename** | Communications and Operation Management Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Communications and Operation Management Policy |
| **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 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.

## 2 Purpose

This policy covers the key areas in day to day operations management of the Council's IT services.

This policy exists to protect the information and IT Infrastructure owned by Redditch Borough Council and to ensure people are aware of any restrictions in their use.

## 3 Scope

This policy applies to all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council with access to Redditch Borough Council's IT facilities and equipment. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

## 4 Definition

This policy should be applied whenever users access Redditch Borough Council's IT facilities and equipment, and especially when managing, developing, configuring or maintaining Redditch Borough Council's IT facilities and equipment.

Local procedures, standards and work instructions may be defined in the appendices to allow flexibility of organisational practices. This policy provides a minimum requirement to be met under nationally recognised standards.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.].
    - Malware and malicious and mobile code.
    - Information leakage.
    - Un-authorised changes

# 6 Applying the Policy

## 6.1 Operational Procedures and Responsibilities

### 6.1.1 Documented Operating Procedures

Operating procedures are used in all day to day maintenance of Redditch Borough Council IT systems and infrastructure in order to ensure the highest possible service from these assets. These operating procedures must be documented to an appropriate level of detail for the departmental team that will be using them.

### 6.1.2 Change Management

Changes to the Council's operational systems must be controlled with a formally documented change control procedure. The change control procedure should include references to:

- A description of the change and business reasons.
- Information concerning the testing phase.
- Impact assessment including security, operations and risk.
- Formal approval process.
- Communication to all relevant people of the changes.
- Procedures for aborting and rolling back if problems occur.
- Process for tracking and audit.

All significant changes to the main infrastructure (e.g. Network, Directories) need to be assessed for their impact on information security as part of the standard risk assessment.

### 6.1.3 Separation of Development, Test and Operational Facilities[1]

- The development and test environments will be separate from the live operational environment to reduce the risk of accidental changes or unauthorised access.

## 6.2 System Planning and Acceptance

### 6.2.1 Capacity Planning

All Redditch Borough Council IT infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key IT infrastructure components include, but are not restricted to, the following:

- File servers.
- Domain servers.
- E-mail servers.
- Web servers.
- Printers.
- Networks.
- Environmental controls including air conditioning.

[1] This should include reference to authorisation levels and references to 3rd party capabilities

### 6.2.2 System Acceptance

All departments must inform ICT via the Helpdesk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through the ICT.

New information systems, product upgrades, patches and fixes must all undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorisation.

3rd party applications must also be monitored for service packs and patches.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

## 6.3 Protection against Malicious and Mobile Code

Appropriate steps are taken to protect all Redditch Borough Council IT systems, infrastructure and information against malicious code. Effective and up-to-date anti-virus software is run on all servers and PCs. Redditch Borough Council staff are responsible for ensuring that they do not introduce malicious code into Redditch Borough Council IT systems – as stated within the Software Policy.

Where a virus is detected on a Redditch Borough Council system, the individual must contact the ICT Helpdesk.

### 6.3.1 Patching

All servers must have appropriate critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. Patches must be applied to all software on the Council network where appropriate.

Unpatchable software must not be used where there is a GCSx connection provided.

There must be a full record of which patches have been applied and when.

### 6.3.2 Controls against Malicious and Mobile Code

In order to prevent malicious and mobile code, appropriate access controls (e.g. administration / user rights) shall be put in place to prevent installation of software by all users.

Requests for software installation shall only be accepted where there is a clear technical verification.

Anti-malware software will be installed on appropriate points on the network and on hosts.

### 6.3.3 Examples of Malicious and Mobile Code

Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:

- ActiveX.
- Java.
- JavaScript.
- VBScript.
- Macros.
- HTTPS.
- HTML.

## 6.4 Backups

### 6.4.1 Information Backup

Regular backups of essential business information must be taken to ensure that the Council can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented.
Any 3rd parties that store Council information must also be required to ensure that the information is backed up.

Full backup documentation, including a complete record of what has been backed up along with the recovery procedure, must be stored at an off site location in addition to the copy at the main site and be readily accessible. This must also be accompanied by an appropriate set of media tapes and stored in a secure area. The remote location must be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

### 6.4.2 Information Restore

Full documentation of the recovery procedure must be created and stored. Regular restores of information from back up media must be tested to ensure the reliability of the back up media and restore process and this should comply with the agreed change management process.

## 6.5 Storage Media Handling

Storage media includes, but is not restricted, to the following:

- Computer Hard Drives (both internal and external).
- CDs.
- DVDs.
- Optical Disks
- USB Memory Sticks
- Media Card Readers.
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

### 6.5.1 Management of Removable Media

Removable computer media (e.g. tapes, disks, cassettes and printed reports) must be protected to prevent damage, theft or unauthorised access.

Documented procedures must be kept for backup tapes that are removed on a regular rotation from Council buildings. Media stores must be kept in a secure environment. Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

For further information, please refer to Removable Media Policy.

### 6.5.2 Physical Storage Media in Transit

Storage media being transported must be protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate, physical controls such as encryption or special locked containers should also be used.

For further information, please refer to Removable Media Policy.

### 6.5.3 Disposal of Storage Media

Storage media that is no longer required must be disposed of safely and securely to avoid data leakage.

Any previous contents of any reusable storage media that are to be removed from the Council must be erased. This must be a thorough removal of all data from the storage media to avoid the potential of data leakage.

For further information, please refer to Removable Media Policy.

### 6.5.4 Security of System Documentation

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by ICT staff. This does not include generic manuals that have been supplied with software. Examples of the documentation to be protected include, but are not restricted to, descriptions of:

- Applications.
- Processes.
- Procedures.
- Data structures.
- Authorisation details.

Effective version control should be applied to all documentation and documentation storage.

## 6.6 Monitoring

### 6.6.1 Audit Logging for Restricted Data and GCSx Services

Audit logs must be kept for a minimum of six months which record exceptions and other security related events[2]. As a minimum audit logs must contain the following information:

- System identity.
- User ID.
- Successful/Unsuccessful login.
- Successful/Unsuccessful logoff.

[2] It is good practice to keep all audit logs for 6 months

- Unauthorised application access.
- Changes to system configurations.
- Use of privileged accounts (e.g. account management, policy changes, device configuration).

Access to the logs must be protected from unauthorised access that could result in recorded information being altered or deleted.
Where appropriate, classified data should be stored separately from non-classified data. Data sent or received via GCSx must be stored separately from non-classified data.

### 6.6.2 Administrator and Operator Logs

Operational staff and system administrators must maintain a log of their activities. The logs should include.

- Back-up timings and details of exchange of backup tapes.
- System event start and finish times and who was involved.
- System errors (what, date, time) and corrective action taken.

The logs should be checked regularly to ensure that the correct procedures are being followed.

### 6.6.3 Clock Synchronisation

All computer clocks must be synchronised to the GSI time source to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation.

## 6.7 Network Management

### 6.7.1 Network Controls

Connections to the Redditch Borough Council network infrastructure are made in a controlled manner. Network management is critical to the provision of Council services and must apply the following controls:

- Operational responsibility for networks should, where possible be separate from computer operations activities.
- There must be clear responsibilities and procedures for the management of remote equipment and users (please refer to the Remote Working Policy and Removable Media Policy).
- Where appropriate, controls must be put in place to protect data passing over the network (e.g. encryption).

The network architecture must be documented and stored with configuration settings of all the hardware and software components that make up the network. All components of the network should be recorded in an asset register.

All hosts must be security hardened to an appropriate level. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

### 6.7.2 Wireless Networks

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption must be used on the network to prevent information being intercepted. WPA2 should be applied as a minimum.

### 6.8 Systems Development and Maintenance

#### 6.8.1 Protection of System Test Data

If personal information is used during the development and test phase of preparing application software it must be protected and controlled in line with the Data Protection Act (please refer to the Legal Responsibilities Policy) and where possible depersonalised. If operational data is used controls must be used including, but not limited to, the following:

- An authorisation process.
- Removal of all operational data from the test system after use.
- Full audit trail of related activities.
- Any personal or confidential information must be protected as if it were live data.

### 6.9 Annual Health Check

An annual health check of all Council IT infrastructure systems and facilities must be undertaken by ICT every 12 months. This health check must include, but is not restricted to, the following:

- A full penetration test.
- A network summary that will identify all IP addressable devices.
- Network analysis, including exploitable switches and gateways.
- Vulnerability analysis, including patch levels, poor passwords and services used.
- Exploitation analysis.
- A summary report with recommendations for improvement.

## 7 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 ICT via the Helpdesk.

## 8 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, councillors, all temporary staff, all contractors etc |

## 9 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 ICT Transformation Manager.

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Software Policy.
- Remote Working Policy.
- Removable Media Policy.
- Legal Responsibilities Policy.
- IT Infrastructure Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Email Policy.
- Internet Acceptable Usage Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- IT Access Policy.
- Computer, Telephone and Desk Use Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.

## 11 Key Messages

- Changes to the Council’s operating systems must be 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.

# Policy Document

# Computer, Telephone and Desk Use Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Computer, Telephone and Desk Use Policy |
| **Author** | Mark Hanwell |
| **Filename** | Computer Telephone and Desk Use Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Computer, Telephone and Desk Use Policy |
| **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 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.

## 2 Purpose

Modern day business operations and advances in technology have necessitated the wide spread use of computer facilities into most offices within Redditch Borough Council and, with the advent of portable computers, away from the Council's premises.

As such, there is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for the pursuance of personal interests or for amusement/entertainment. The Council also handles large amounts of PROTECT and RESTRICTED information. The security of this information is of paramount importance. Ensuring that a clear desk policy operates across the Council can help prevent the security of this information from being breached.

The misuse of Redditch Borough Council 's computer and telephony resources is considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action including dismissal.

The purpose of this document is to establish guidelines as to what constitutes "computer and telephony resources", what is considered to be "misuse" and how users should operate within a clear desk environment.

## 3 Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to information systems or information used for Redditch Borough Council purposes.

This policy should be read in conjunction with the following policies:

- Email Acceptable Use Policy.
- Internet Acceptable Use Policy.
- Software Policy.
- Legal Responsibilities Policy.

## 4 Definition

This policy should be applied whenever users who access information systems or information utilise Redditch Borough Council 's computer and telephony resources.

Computer and telephony resources include, but are not restricted to, the following :

- Departmental computers.
- Personal computers.
- Portable laptop computers.
- Printers.
- Network equipment.
- Telecommunications facilities.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

### 6.1 Computer Resources Misuse

No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case will need to be taken into account. However, some examples are outlined below :

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- Storing/loading/executing of software that has not been authorised by ICT.
- Storing/loading/executing of software:
    - that has not been acquired through approved Council procurement procedures, or
    - for which the Council does not hold a valid program licence, or
    - that has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose which is not work related.

For further information, users are requested to read the following policies:

- Email Policy.
- Internet Acceptable Use Policy.
- Software Policy.

### 6.2 Telephone

Redditch Borough Council has an Acceptable Use Policy / Code of Practice relating to telephone use. This relates to the use of Council owned static and mobile telephones for private telephone calls and must be adhered to at all times.

The Council acknowledges that employees may need to make calls of a personal nature whilst at work. This Code of Practice outlines reasonable steps that all employees are expected to take to ensure that the provision of service is not compromised and there is no financial loss.

1. Where possible, private calls should be made outside working hours.

2. Private calls during these hours should be kept to a minimum, so as not to prevent business calls getting through.

3. There may be times when unforeseen working commitments may require the rearranging of personal engagements. The Council recognises that such calls are necessary in order for employees to effectively perform their duties. However, the Council stresses that such calls are normally exceptional, and expect employees to recognise when such calls are required.

The misuse of Redditch Borough Council's telephone services is also considered to be potential gross misconduct and may render the individual(s) concerned liable to disciplinary action.

### 6.3 Clear Desk

Redditch Borough Council has a clear desk policy in place in order to ensure that all information is held securely at all times. Work should not be left on desks unattended and should be removed from view when unsupervised.

At the end of each day, every desk will be cleared of all documents that contain any Redditch Borough Council PROTECT or RESTRICTED information, or any information relating to clients or citizens.

Redditch Borough Council PROTECT or RESTRICTED information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

Users of IT facilities are responsible for safeguarding data by ensuring that equipment is locked when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Computer screens must be locked to prevent unauthorised access when unattended and screens will lock automatically after a 15 minute period of inactivity, in order to protect information. A screen saver with password protection enabled will be used on all PCs. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action.

### 6.4 Legislation

Users should understand the relevant legislation relating to Information Security and Data Protection, and should be aware of their responsibilities under this legislation. The following statutory legislation governs aspects of the Council's information security arrangements. This list is not exhaustive:

- The Freedom of Information Act 2000.
- The Data Protection Act 1998.
- The Computer Misuse Act 1990.

Individuals can be held personally and legally responsible for breaching the provisions of the above and other Acts.

## 7 Policy Compliance

If any user is found to have breached this policy, they will 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.

## 8 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 |

## 9 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..

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- IT Access Policy.
- Remote Working Policy.
- Removable Media Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.
- Communications and Operation Management Policy.

## 11 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 wherever possible and in accordance with this policy.
- Redditch Borough Council PROTECT or RESTRICTED information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# Policy Document

# Email Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Email Policy |
| **Author** | Mark Hanwell |
| **Filename** | Email Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Email Policy |
| **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 Policy Statement

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

## 2 Purpose

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

## 3 Scope

This policy covers all email systems and facilities that are provided by Redditch Borough Council for the purpose of conducting and supporting official business activity through the Councils network infrastructure and all stand alone and portable computer devices.

This policy is intended for all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of email facilities.

The use of email facilities will be permitted only by staff that have been specifically designated as authorised users for that purpose, received appropriate training and have confirmed in writing that they accept and agree to abide by the terms of this policy.

The policy also applies where appropriate to the internal Microsoft exchange e-mail facility which may be accessed by staff who are not authorised Internet and e-mail users.

The use of email facilities by staff that have not been authorised for that purpose will be regarded as a disciplinary offence.

## 4 Definition

All email prepared and sent from Redditch Borough Council email addresses or mailboxes, and any non-work email sent using Redditch Borough Council ICT facilities is subject to this policy.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

## 6 Applying the Policy

### 6.1 Email as Records

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. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email (please also refer to section 6.7). All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Redditch Borough Council business should be considered to be an official communication from the Council. In order to ensure that Redditch Borough Council is protected adequately from misuse of e-mail, the following controls will be exercised:

i. It is a condition of acceptance of this policy that users comply with the instructions given during the email training sessions.
ii. All official external e-mail must carry the following disclaimer:

> *"*************************************************************
>
> *This email and any files transmitted with it are intended solely for the use of the individual to whom it is addressed. If you have received this email in error any use, dissemination, forwarding or copying of this e-mail is prohibited. If you have received this email in error please notify the ICT Helpdesk via an e-mail to helpdesk@Bromsgroveandredditch.gov.uk including a copy of this message. Please then delete this email and destroy any copies of it.*
>
> *Statements and opinions expressed are those of the author and do not necessarily represent those of the Authority. The content of this email is not*

> *legally binding unless confirmed by us in a signed letter. Redditch Borough Council has taken every reasonable precaution to minimise the risk of software viruses being contained in attachments to this e-mail. You should, however, carry out your own virus checks before opening the attachment(s). Redditch Borough Council will not be liable for direct, special, indirect or consequential damages arising from alteration of the contents of this message by a third party or as a result of any virus being passed on.*
>
> *All Redditch Borough Council emails may be subject to recording and/or monitoring in accordance with relevant legislation.*
>
> *Any Freedom of Information requests should be sent directly to foi@redditchbc.gov.uk*
>
> *************************************************.”

Whilst respecting the privacy of authorised users, Redditch Borough Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council’s ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from Data Protection Officer.

### 6.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or PROTECT or RESTRICTED information or of communicating in the particular circumstances.

All emails sent to conduct or support official Redditch Borough Council business must comply with corporate communications standards. Redditch Borough Council’s Communications Policy must be applied to email communications.

Councillors must ensure that any emails containing sensitive information must be sent from an official council email. Any emails containing PROTECT or RESTRICTED information must be sent from a GCSx email.

Email must not be considered to be any less formal than memo’s or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council’s reputation or its relationship with customers, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of PROTECT or RESTRICTED material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.

### 6.3 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Redditch Borough Council systems or facilities.

### 6.4 Mail Box Size

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 30MB in size – files in excess of this will be stopped and only released following individual approval.

### 6.5 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that Redditch Borough Council:

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.

Monitoring of content will only be undertaken by staff specifically authorised for that purpose in accordance with Communications and Operation Management Policy. These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business.

Where a manager suspects that the email facilities are being abused by a user, they should contact their line manager or the ICT Transformation Manager. Designated staff in ICT can investigate and provide evidence and audit trails of access to systems. ICT will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by request of their line manager for specific work purposes whilst they are absent. If this is the case a written request to the Head of Service is required. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the employee. Authorised staff must only open emails which are relevant.

### 6.6 Security

Emails sent between Bromsgroveandredditch.gov.uk address are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, PROTECT and RESTRICTED material must not be sent via email outside a closed network, 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 and RESTRICTED material.

**All Council employees that require access to GCSx email must read, understand and sign the GCSx Acceptable Usage Policy and Personal Commitment Statement.**

### 6.7 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure of whether they should pass on information, they should consult their line manager.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of RedditchBc.

Care should be taken when addressing all emails, but particularly where they include PROTECT or RESTRICTED information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent PROTECT or RESTRICTED material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact ICT in the first instance.

The automatic forwarding of a GCSx email to a lower classification email address (i.e. a standard .gov.uk email) contradicts national guidelines and is therefore not acceptable.

### 6.8 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Redditch Borough Council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to ICT.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to the ICT helpdesk.
- Must report any suspected files to the ICT helpdesk.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

## 7 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.

## 8 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 |

## 9 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.

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Software Policy.
- Communications and Operation Management Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Internet Acceptable Usage Policy.
- IT Access Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Removable Media Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.

## 11 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 (see section 6.1).
- 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.

Page 144

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Policy Document

# GCSx Acceptable Usage Policy and Personal Commitment Statement

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | GCSx AUP and Personal Commitment Statement |
| **Author** | Mark Hanwell |
| **Filename** | GCSx AUP and Personal Commitment Statement.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | GCSx AUP and Personal Commitment Statement Policy |
| **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 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.

## 2 Purpose

GCSx stands for Government Connect Secure Extranet. It is a secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations that sit on the pan-government secure network infrastructure.

Some Council staff will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include staff having access to a secure email facility. All staff requiring access to the GCSx network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement.

This policy and statement does not replace the Council's existing acceptable usage, or any other, policies. It is a supplement to them.

## 3 Scope

All users of the GCSx connection must be aware of the commitments and security measures surrounding the use of this network. This policy must be adhered to by all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council using the GCSx facilities.

## 4 Definition

This policy must be adhered to at all times when accessing GCSx facilities.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 GCSx Acceptable Usage Policy

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

- I understand and agree to comply with the security rules of my organisation.

For the avoidance of doubt, the security rules relating to secure e-mail and information systems usage include:

1. I acknowledge that my use of the GCSx may be monitored and/or recorded for lawful purposes.

2. I agree to be responsible for any use by me of the GCSx using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and,

3. will not use a colleague's credentials to access the GCSx and will equally ensure that my credentials are not shared and are protected against misuse; and,

4. will protect such credentials at least to the same level of secrecy 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); and,

5. will not attempt to access any computer system that I have not been given explicit permission to access; and,

6. will not attempt to access the GCSx other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose; and,

7. will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry; and,

8. will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and,

9. will not make false claims or denials relating to my use of the GCSx (e.g. falsely denying that an e-mail had been sent or received); and,

10. will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material; and,

11. will appropriately label, using the HMG Security Policy Framework (SPF), information up to RESTRICTED sent via the GCSx; and,

12. will not send PROTECT or RESTRICTED information over public networks such as the Internet; and,

13. will always check that the recipients of e-mail messages are correct so that potentially sensitive or PROTECT or RESTRICTED information is not accidentally released into the public domain; and,

14. will not auto-forward email from my GCSx account to any other non-GCSx email account; and,

15. will not forward or disclose any sensitive or PROTECT or RESTRICTED material received via the GCSx 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; and,

16. will seek to prevent inadvertent disclosure of sensitive or PROTECT or RESTRICTED information by avoiding being overlooked when working, by taking care when printing information received via GCSx (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; and,

17. will securely store or destroy any printed material; and,

18. will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via GCSx (this will be in accordance with the Computer, Telephone and Desk Use Policy - e.g. logging-off from the computer, activate a password-protected screensaver etc, so as to require a user logon for activation); and,

19. where ICT Services has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection; and,

20. will make myself familiar with the Council's security policies, procedures and any special instructions that relate to GCSx; and,

21. will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security Information Security Incident Management Policy; and,

22. will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and,

23. will not remove equipment or information from council premises without appropriate approval; and,

24. will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft) in accordance with the Council's Remote Working Policy; and,

25. will not introduce viruses, Trojan horses or other malware into the system or GCSx; and,

26. will not disable anti-virus protection provided at my computer; and,

27. will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that the Council informs me are relevant (please refer to the Legal Responsibilities Policy); and,

28. if I am about to leave the Council, I will inform my manager prior to departure of any important information held in my account and manage my account in accordance with the Council's email and records management policy.

| | |
|---|---|
| Document Date: | |
| Name of User: | |

| | |
|---|---|
| Position: | |
| Department: | |
| User Access Request Approved by: | |
| User Access Request Approved by: | |
| Username Allocated | |
| Email Address Allocated: | |
| User Access Request Processed: | |

## 7 GCSx Personal Commitment Statement

I, [________________], accept that I have been granted the access rights to GCSx. I understand and accept the rights which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this policy, personal commitment statement, and all other ICT policies. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Council's disciplinary policy.

Signature of User: ……………………………………………………………….

A copy of this agreement is to be retained by the member of staff and Human Resources.

## 8 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.

## 9 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 |

## 10 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.

## 11 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document.

- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Email Policy
- Internet Acceptable Usage Policy.
- Software Policy.
- IT Access Policy.
- Removable Media Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.
- IT Infrastructure Policy.

# Policy Document

# Human Resources Information Security Standards

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Human Resources Information Security Policy |
| **Author** | Mark Hanwell |
| **Filename** | Human Resources Information Security.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Human Resources Information Security Policy |
| **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 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.

## 2 Purpose

Redditch Borough Council holds large amounts of personal and RESTRICTED information. Information security is very important to help protect the interests and confidentiality of the Council and its customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

The procedures accompanying this policy are split into 3 key stages of a user's access to information or information systems used to deliver Council business:

1. Prior to granting access to information or information systems - checks must be made to ensure that the individual is suitable for access to Council information systems.
2. The period during access to information or information systems - users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure it remains appropriate.
3. When a user's requirement for access to information or information systems ends (i.e. when a user terminates their employment with the Council, or changes their role so that access is no longer required) - access needs to be removed in a controlled manner.

This policy also addresses third party access to Council information systems (e.g. contractors, service providers, voluntary agencies and partners).

## 3 Scope

This policy applies to any person that requires access to Council information systems or information of any type or format (paper or electronic).

The policy applies automatically to all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council.

Where access is to be granted to any third party (e.g. contractors, service providers, voluntary agencies, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with the Council employee that initiates this third party access.

## 4 Definition

Redditch Borough Council understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Council information systems **must**:

- Be suitable for their roles.

- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any user's access to information or information systems used to deliver Council business.

Access to Council information systems will not be permitted until the requirements of this policy have been met.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

## 7 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.

## 8 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 |

## 9 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

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- IT Access Policy.
- Information Protection Policy.
- Information Security Incident Management Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy;

- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Removable Media Policy.
- Legal Responsibilities Policy.
- Communications and Operation Management Policy.
- IT Infrastructure Policy.

## 11 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.

## Appendix 1

## A1 Applying the Policy – Prior to Access to Information or Information Systems

### A1.1 Prior to Employment

The Council must ensure that potential users are recruited in line with the Council's Recruitment and Selection Policy for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those users. These requirements are corporate in nature

### A1.2 Roles and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the Information Asset Owner – please refer to the Information Protection Policy.

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the ICT. Helpdesk in a timely manner, using an agreed process.

The information security responsibilities of users must be defined and documented and incorporated into induction processes and contracts of employment. As a minimum this will include:

- A statement that every user is aware of, and understands, the following Council 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.

### A1.3 User Screening

Background verification checks must be carried out on all potential users, in accordance with all relevant laws, regulations and ethics. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.

The basic requirements for Council employment must be:

- Minimum of two satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or equivalent document that contains a photograph.

Users who require access to PROTECT and RESTRICTED information and / or require use of the Government Connect Secure Extranet (GCSx) and email facility **must** be cleared to "Baseline Personnel Security Standard". The following requirements **must** be met:

- Minimum of 2 satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.

- Identity check against a passport or equivalent document that contains a photograph. Identity must be proven through visibility of:
    - A full 10 year passport.
- Or two from the following list:
    - British driving licence.
    - P45 form.
    - Birth certificate.
    - Proof of residence – i.e. council tax or utility bill.
- Verification of full employment history for the past 3 years.
- Verification of nationality and immigration status.
- Verification of criminal record (unspent convictions only).

Criminal Records Bureau checks on the user must be carried out to an appropriate level as demanded by law.

Where access is to systems processing payment card data, credit checks on the user must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

All the above requirements for verification checks must be applied to technical support and temporary staff that have access to those systems or any copies of the contents of those systems (e.g. backup tapes, printouts, test data-sets).

### A1.4 Terms and Conditions of Employment

As part of their contractual obligation users must agree and sign the terms of their employment contract, which shall state their and the Council's responsibilities for information security. This must be drafted by the Council's lawyers and must form an integral part of the contract of employment.

Each user must sign a confidentiality statement that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

## A2 Applying the Policy – During Access to Information or Information Systems

### A2.1 During Continued Employment

The Council must ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their work, and to reduce the risk of human error. It is also necessary that user changes in role or business environment are carried out in an orderly manner that ensures the continuing security of the information systems to which they have access.

### A2.2 Management Responsibilities

Line managers must notify the appropriate function in a timely manner of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate. Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to user access must be made in a timely manner and be clearly communicated to the user.

Departmental managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate Council policies. These policies include:

- Information Protection Policy.
- Information Security Incident Management Policy.

This requirement must be documented.

### A2.3 Information Security Awareness, Education and Training

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.

It is the role of Departmental managers to ensure that their staff are adequately trained and equipped to carry out their role efficiently and securely.

## A3 Applying the Policy – When Access to Information or Information Systems is No Longer Required

### A3.1 Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to Redditch Borough Council information assets is removed in a timely manner when no longer required by the user.

### A3.2 Termination Responsibilities

Line managers must notify the ICT Helpdesk in a timely manner of the impending termination or suspension of employment so that their access can be suspended.

ICT Helpdesk must notify the appropriate system owners who must suspend access for that user at an appropriate time, taking into account the nature of the termination.

Responsibilities for notifying changes, performing employment termination or change of employment must be clearly defined and assigned.

### A3.3 Return of Assets

Processes must be implemented to ensure that users return all of the organisation's assets in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

### A3.4 Removal of Access Rights

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.

Processes and responsibilities must be agreed and implemented to enable emergency suspension of a user's access when that access is considered a risk to the Council or its systems as defined in the Information Security Incident Management Policy.

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# Policy Document

# Information Protection Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Information Protection Policy |
| **Author** | Mark Hanwell |
| **Filename** | Information Protection Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Information Protection Policy |
| **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 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.

## 2 Purpose

Information is a major asset that Redditch Borough Council has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Council maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at Redditch Borough Council. The policy specifies the means of information handling and transfer within the Council.

## 3 Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Council's information systems. This includes all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Redditch Borough Council purposes.

## 4 Definition

This policy should be applied whenever Council Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Recorded speech.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

## 7 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.

## 8 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 |

## 9 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

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Removable Media Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- IT Access Policy.
- Legal Responsibilities Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.
- IT Infrastructure Policy.
- Document retention and disposal policy

## 11 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.

## Appendix 1

## A1 Applying the Policy

### A1.1 Information Asset Management

### A1.1.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

The Council must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

### A1.1.2 Classifying Information

On creation, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled in accordance with the HMG Security Policy Framework (SPF). The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification. Information up to RESTRICTED sent via GCSx must be labelled appropriately using the SPF guidance.

The SPF requires information assets to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependant on this scheme.

The classes are:

- Unclassified.
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.
- TOP SECRET.

### Personal Information

Personal information is any information about any living, identifiable individual. The Council is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998. Details of specific requirements can be found in the Legal Responsibilities Policy.

### A1.1.3 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

### A1.1.4 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done

### A1.1.6 Corporate Information Assets

For information assets whose use throughout the Council is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

### A1.1.7 Acceptable Use of Information Assets

The Council must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council and use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

As a minimum this will include:

- Email Policy.
- Internet Acceptable Usage Policy.
- Computer and Telephone Misuse Policy.
- Software Policy.
- Remote Working Policy.
- Removable Media Policy.

## A1.2 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Records management and retention guidance will be followed

Staff should not be allowed to access information until their line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

Databases holding personal information will have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information.

Files which are identified as a potential security risk should only be stored on secure network areas

## A1.3 Disclosure of Information

### A1.3.1 Sharing PROTECT or RESTRICTED Information with other Organisations

PROTECT or RESTRICTED information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

Disclosing PROTECT or RESTRICTED information to any external organisation is also **prohibited**, unless via the Government Connect Secure Extranet (GCSx) email. Emails sent between Bromsgroveandredditch.gov.uk addresses are held within the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system.

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. For further information see the Email Policy.

An official email legal disclaimer must be contained with any email sent. This can be found in the Email Policy.

The disclosure of PROTECT or RESTRICTED information in any way other than via GCSx email is a disciplinary offence. If there is suspicion of a Councillor or employee treating PROTECT or RESTRICTED information in a way that could be harmful to the Council or to the data subject, then it is be reported to the ICT Transformation Manager, and the person may be subject to disciplinary procedure.

Any sharing or transfer of Council information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

# Policy and Procedure Document

# Information Security Incident Management Policy and Procedure

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Information Security Incident Management Policy |
| **Author** | Mark Hanwell |
| **Filename** | Information Security Incident Management Policy. doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Information Security Incident Management Policy |
| **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 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.

## 2 Purpose

The aim of this policy is to ensure that Redditch Borough Council reacts appropriately to any actual or suspected security incidents relating to information systems and data.

## 3 Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who use Redditch Borough Council IT facilities and equipment, or have access to, or custody of, customer information or Redditch Borough Council information.

All users **must** understand and adopt use of this policy and are responsible for ensuring the safety and security of the Council's systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

## 4 Definition

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Procedure for Incident Handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the ICT helpdesk. The ICT Helpdesk enables ICT to identify when a series of events or weaknesses have escalated to become an incident. It is vital for ICT to gain as much information as possible from the business users to identify if an incident is occurring.

## 7 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.

## 8 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 |

## 9 Review and Revision

This policy, and all related appendices, 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.

## 10 References

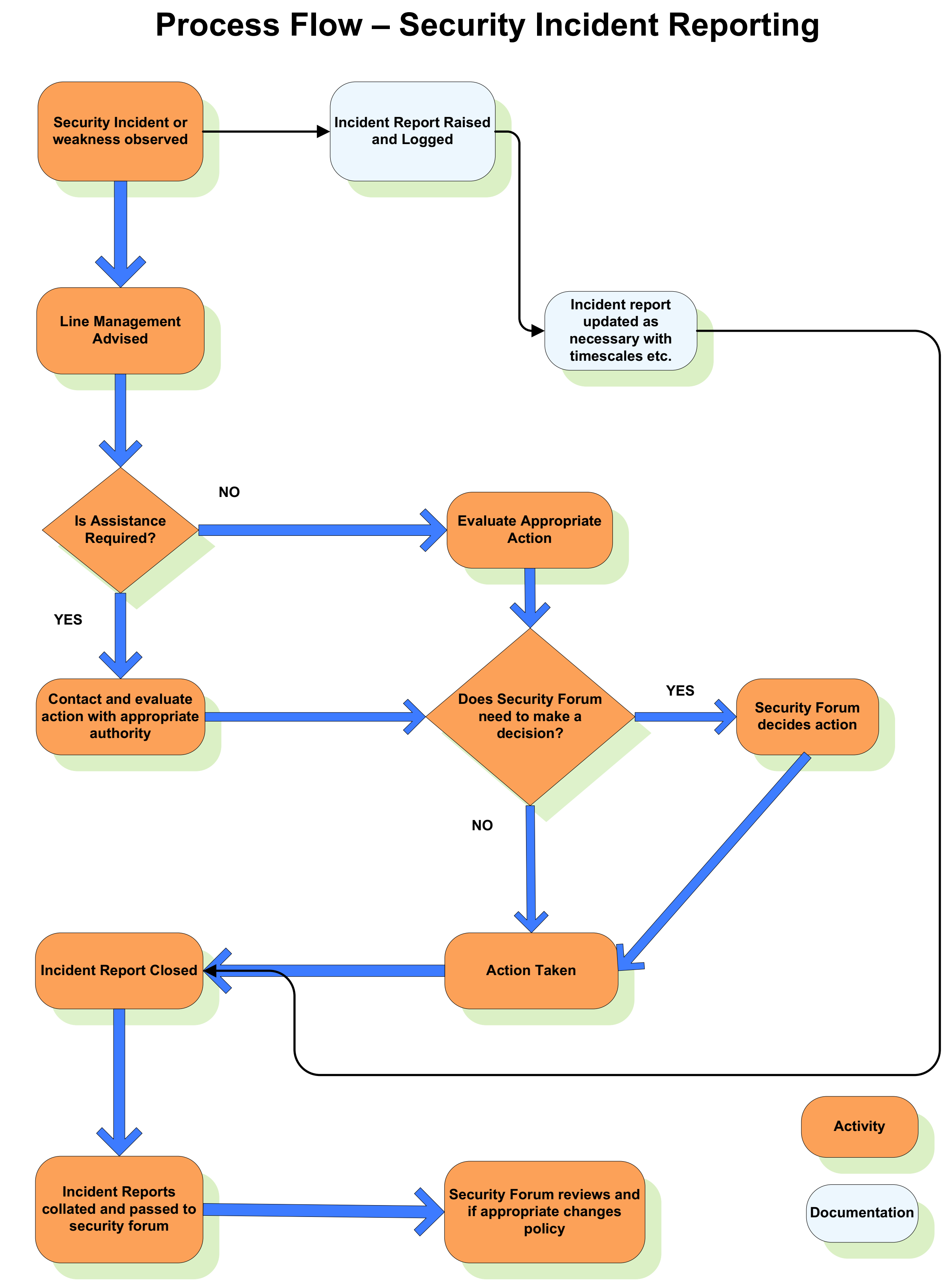
The following Redditch Borough Council policy documents are directly relevant to this policy:

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

## 11 Key Messages

- All staff should report any incidents or suspected incidents immediately by reporting them to the ICT helpdesk.
- We can maintain your anonymity when reporting an incident if you wish.
- If you are unsure of anything in this policy you should ask for advice from your line manager or ICT.

## 12 Appendix 1 – Process Flow; Reporting an Information Security Event or Weakness


Process Flow – Security Incident Reporting
Security Incident or weakness observed
Incident Report Raised and Logged
Line Management Advised
Incident report updated as necessary with timescales etc.
Is Assistance Required?
NO
Evaluate Appropriate Action
YES
Contact and evaluate action with appropriate authority
Does Security Forum need to make a decision?
YES
Security Forum decides action
NO
Incident Report Closed
Action Taken
Activity
Incident Reports collated and passed to security forum
Security Forum reviews and if appropriate changes policy
Documentation

## 13 Appendix 2 – Examples of Information Security Incidents

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

**Malicious**

- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive e-mail to 'all staff'.
- Receiving solicited mail of an offensive nature.
- Receiving solicited mail which requires you to enter personal data.
- Changing data without authorisation.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others other than the ICT helpdesk.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

- Use of unapproved or unlicensed software on Redditch Borough Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

**Theft / Loss**

- Theft / loss of a hard copy file through negligence.
- Theft / loss of any Redditch Borough Council computer equipment e.g. laptops, memory sticks and CDs through negligence.

## 14 Appendix 3 - Procedure for Incident Handling

Please report all incidents to help.desk@redditchbc.gov.uk

### 14.1 Reporting Information Security Events or Weaknesses

The following sections detail how people must report information security events or weaknesses. Appendix 1 provides a process flow diagram illustrating the process to be followed when reporting information security events or weaknesses.

#### 14.1.1 Reporting Information Security Events for all Employees

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to your line manager and the Information Manager for the impact to be assessed.

All suspected security events should be reported immediately to the ICT Helpdesk.

The ICT Helpdesk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information should be supplied:

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

#### 14.1.2 Collection of Evidence

Upon a potential incident the authority may need to collect evidence. This could include all data for example personal information, deleted files, and emails from any equipment owned by Redditch Borough Council.

Page 182

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# 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.

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Policy Document

# Internet Acceptable Usage Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Internet Acceptable Usage Policy |
| **Author** | Mark Hanwell |
| **Filename** | Internet Acceptable Usage Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Internet Acceptable Usage Policy |
| **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 Policy Statement

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

## 2 Purpose

This policy document tells you how you should use your Council Internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

This policy replaces all locally agreed Internet usage policies.

## 3 Scope

This Internet Acceptable Usage Policy applies to, but is not limited to, all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who access the Councils Internet service and IT equipment.

## 4 Definition

This Internet Acceptable Usage Policy should be applied at all times whenever using the Council provided Internet facility. This includes access via any access device including a desktop computer or a smartphone device.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

### 6.1 What is the Purpose of Providing the Internet Service?

The Internet service is primarily provided to give Council employees and Councillors:

- Access to information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained web sites.
- An electronic commerce facility.

### 6.2 What You Should Use Your Council Internet For

Your Council Internet should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to and/or provision of information.
- Research.
- Electronic commerce

### 6.3 Personal Use of the Council's Internet Service

At the discretion of your line manager, and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for example during your lunch-break).

The Council is not, however, responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Council's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

You should ensure that personal goods and services purchased are not delivered to Council property. Rather, they should be delivered to your home or other personal address.

If you are in any doubt about how you may make personal use of the Council's Internet Service you are advised not to do so.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Redditch Borough Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

### 6.4 Internet Account Management, Security and Monitoring

The provision of Internet access is owned by the Council and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity.
- The filtering system monitors and records all access for reports that are produced for line managers and auditors.

### 6.5 Things You Must Not Do

Access to the following categories of websites is currently blocked using a URL filtering system :

- Adult
- Advertisements
- Alcohol and Tobacco
- Cheating and Plagiarism
- Child Porn
- Cults
- Dating
- File Transfer Services
- Filter Avoidance
- Freeware and Shareware
- Gambling
- Games
- Hacking
- Hate Speech
- Illegal Activities
- Illegal Drugs
- Instant Messages
- Internet Telephony
- Non-Sexual Nudity
- Online Communities
- Online Storage and Backup
- Paranormal and Occult
- Peer File Transfer
- Porn
- Social Networking
- Software Updates
- Streaming Media
- Tasteless or Obscene
- Weapons
- Web Hosting
- Web-based Chat
- Web-based Email

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet access to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter “money making” sites or enter or use “money making” programs.
- Run a private business.
- Download any software that does not comply with the Council’s Software Policy.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

You must not attempt to by-pass or remove any of the security and monitoring facilities.

### 6.6 Your Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the Council's Internet facility within the terms described herein.
- Read and abide by the following related policies :
    - Email Policy.
    - Software Policy.
    - IT Access Policy.
    - Remote Working Policy.
    - Legal Responsibilities Policy.

### 6.7 Line Manager's Responsibilities

It is the responsibility of Line Managers to ensure that the use of the Internet facility:

- Within an employees work time is relevant to and appropriate to the Council's business and within the context of the users responsibilities.
- Within an employees own time is subject to the rules contained within this document.

### 6.8 Whom Should I Ask if I Have Any Questions?

In the first instance you should refer questions about this policy to your Line Manager or ICT.
You should also refer technical queries about the Council's Internet service to the ICT Services Helpdesk.

### 6.9 Acceptable Usage Policy

Each user must read, understand and sign to verify they have read and accepted this policy. This policy must be signed annually.

- I understand and agree to comply with the Internet Acceptable Usage Policy of my organisation.

Signature of User: …………………………………………………………………….

Print name: ………………………………………. Date:………………………….

A copy of this agreement is to be retained by the User and ICT.

## 7 Policy Compliance

If any user is found to have breached this policy, they will 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.

## 8 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 |

## 9 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.

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Software Policy.
- IT Access Policy.
- Remote Working Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy;

- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.
- Communications and Operation Management Policy.

## 11 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 personal use of the Internet in your own time (for example during your lunch-break).
- 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.
- You must not allow anyone else to use your internet access.

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Policy Document

# IT Access Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | IT Access Policy |
| **Author** | Mark Hanwell |
| **Filename** | IT Access Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | IT Access Policy |
| **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 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.

## 2 Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Redditch Borough Council which must be managed with care. All information has a value to the Council. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

## 3 Scope

This policy applies to all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to Redditch Borough Council's information and information systems.

## 4 Definition

Access control rules and procedures are required to regulate who can access Redditch Borough Council information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Redditch Borough Council information in any format, and on any device.

## 5 Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

# 6 Applying the Policy - Passwords

## 6.1 Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

### 6.1.1 *Weak* and *strong* passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

## 6.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different Redditch Borough Council systems.
- Do not use the same password for systems inside and outside of work.

## 6.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 42 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the ICT helpdesk.

Users **must not** reuse the same password within 24 password changes .

## 6.4 System Administration Standards

The password administration process for individual Redditch Borough Council systems is well-documented and available to designated individuals.

All Redditch Borough Council IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

## 7 Applying the Policy – Employee Access

### 7.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Redditch Borough Council. Each user must be allocated access rights and permissions to computer systems and data that:

- Are applicable to the tasks they are expected to perform.
- Have a unique login and password that is not shared with or disclosed to any other user.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

### 7.2 User Registration

A request for access to the Council's computer systems must first be submitted to the ICT Helpdesk.. Applications for access must only be submitted if approval has been gained from your line manager.

When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the ICT Helpdesk.

### 7.3 User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing ICT of any changes to their role and access requirements.

### 7.4 Network Access Control

Only equipment approved by ICT can be connected to the Council's network. The normal operation of the network must not be interfered with.

### 7.5 User Authentication for External Connections

Where remote access to the Redditch Borough Council network is required, an application must be made via the ICT Helpdesk. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a Crypto Card.. For further information please refer to the Remote Working Policy.

### 7.6 Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the ICT Helpdesk. Any changes to supplier's connections must be immediately sent to the ICT so that access can be updated or ceased. All permissions and access methods must be controlled by ICT.

Partners or 3rd party suppliers must contact the ICT Helpdesk before connecting to the Redditch Borough Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

### 7.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

### 7.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The departmental administrator of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) above.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.

- Be logged and auditable.

## 8 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.

## 9 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 |

## 10 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.

## 11 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Remote Working Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Email Policy.

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

## 12 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 user ID 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 Helpdesk.
- Partners or 3rd party suppliers must contact the ICT Helpdesk before connecting to the Redditch Borough Council network.

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# Policy Document

# IT Infrastructure Security Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | IT Infrastructure Security Policy |
| **Author** | Mark Hanwell |
| **Filename** | IT Infrastructure Security Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | IT Infrastructure Security Policy |
| **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 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.

## 2 Purpose

The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council's information, in line with section A9 of ISO/IEC/27001.

In order to ensure the continued protection of the personal, confidential and RESTRICTED information that Redditch Borough Council holds and uses, and to comply with legislative requirements, information security best practice, and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Government Connect Secure Extranet (GCSx), access to Redditch Borough Council's information equipment and information must be protected.

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the Council's IT data centre. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. No service should fall below the baseline security standard level of protection required for their teams and locations.

## 3 Scope

All Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council with access to Redditch Borough Council's equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the Council's equipment and the information that they use or manipulate.

## 4 Definition

This policy applies to all users of the Council's owned or leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of information within the custody of the Council.

This policy should be applied whenever a user accesses Council information or information equipment. This policy applies to all locations where information within the custody of the Council or information processing equipment is stored, including remote sites.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

### 6.1 Secure Areas

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g. fire, flood, vandalism.

As an example, access to secure areas such as the data centre and IT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should challenge anyone not wearing a badge. Each department must ensure that doors and windows are properly secured.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A Council ICT employee must monitor all visitors accessing secure IT areas at all times.

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.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately. Please also refer to the IT Access Policy and Human Resources Information Security Standards.

### 6.2 Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from Information Services.

All equipment must have a unique asset number allocated to it. This asset number should be recorded in the Departmental and the IS / IT inventories.

For portable computer devices please refer to the Remote Working Policy.

### 6.3 Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Network cables should be protected by conduit and where possible avoid routes through public areas.

### 6.4 Security of Equipment Off Premises

The use of equipment off-site must be formally approved by ICT. Equipment taken away from Redditch Borough Council premises is the responsibility of the user and should:

- Be logged in and out, where applicable.
- Not be left unattended.
- Concealed whilst transported.
- Not be left open to theft or damage whether in the office, during transit or at home.
- Where possible, be disguised (e.g. laptops should be carried in less formal bags).
- Be encrypted if carrying PROTECT or RESTRICTED information.
- Be password protected.
- Be adequately insured.

Further information can be found in the Removable Media Policy and Remote Working Policy.

Users should ensure, where necessary and required, that insurance cover is extended to cover equipment which is used off site. Users should also ensure that they are aware of and follow the requirements of the insurance policy. Any losses / damage must be reported to the ICT Department and the Insurance Section (if applicable).

Staff should be aware of their responsibilities in regard to Data Protection and be conversant with the Data Protection Act (please refer to the Legal Responsibilities Policy).

### 6.5 Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools. Equipment must be returned to ICT for data removal.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

### 6.6 Delivery and Receipt of Equipment into the Council

In order to confirm accuracy and condition of deliveries and to prevent subsequent loss or theft of stored equipment, the following must be applied:

- Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.
- Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

### 6.7 Regular Audit

There should a duty to audit information security arrangements regularly to provide an independent appraisal and recommend security improvements where necessary.

## 7 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.

## 8 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 |

## 9 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.

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- IT Access Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Remote Working Policy.
- Removable Media Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.

## 11 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 ICT 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.

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Policy Document

# Legal Responsibilities Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Email Policy |
| **Author** | Mark Hanwell |
| **Filename** | Legal Responsibilities.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Legal Responsibilities |
| **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 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.

## 2 Purpose

Redditch Borough Council collects, holds and uses data about people and organisations with whom it deals with in order to conduct its business. This data covers, but is not restricted to, the following:

- Current, past and prospective employees.
- Suppliers.
- Customers.
- Others with whom the Council communicates.

In addition, it may occasionally be required by law to collect and use certain types of personal information to comply with the requirements of government departments.

This policy outlines every user's responsibilities under the Data Protection Act 1998 and other relevant legislation.

## 3 Scope

Any information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer, or recorded on other media. There are safeguards in the Data Protection Act 1998 to ensure that personal information is dealt with correctly.

This policy relates to all personal data held by Redditch Borough Council in any form, and all PROTECT or RESTRICTED information held or processed by the Council. It applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who has access to information held or processed by Redditch Borough Council.

## 4 Definition

Redditch Borough Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998, and other relevant information security legislation. Therefore, the Council will ensure that all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to any information held by or on behalf of the Council are fully aware of, and abide by, their duties and responsibilities under this legislation.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy – Data Protection

### 6.1 Relevant Legislation

The following statutory legislation governs aspects of the Council's information security arrangements. This list is not exhaustive:

| **Legislation** | **Areas Covered** |
|---|---|
| The Freedom of Information Act 2000 | Public access to Council information |
| The Human Rights Act 1998 | Right to privacy and confidentiality |
| The Electronic Communications Act 2000 | Cryptography, electronic signatures |
| The Regulation of Investigatory Powers Act 2000 | Hidden surveillance of staff |
| The Data Protection Act 1998 | Protection and use of personal information |
| The Copyright Designs and Patents Act 1988 | Software piracy, music downloads, theft of Council data |
| The Computer Misuse Act 1990 | Hacking and unauthorised access |
| The Environmental Information Regulations 2004 | Public access to Council information related to the environment |
| The Re-use of Public Sector Information Regulations 2005 | The Council's ability to sell certain data sets for commercial gain |

Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Key records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

### 6.2 What is Personal Data?

Personal data is defined as:

> *"data which relate to a living individual who can be identified:*
> *a) from those data; or,*
> *b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;*

> *and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual[1].”*

### 6.3 What are the Principles of Data Protection?

The Data Protection Act 1998 stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Shall be kept secure - i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Data Protection Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data. Sensitive personal data is defined as:

> *“personal data consisting of information as to:*
>
> *a) the racial or ethnic origin of the data subject,*
> *b) his political opinions,*
> *c) his religious beliefs or other beliefs of a similar nature,*
> *d) whether he is a member of a trade union,*
> *e) his physical or mental health or condition,*
> *f) his sexual life,*
> *g) the commission or alleged commission by him of any offence, or*
> *h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.[1]”*

The data subject also has rights under the Data Protection Act. These consist of:

- The right to be informed that processing is being undertaken;
- The right of access to one’s personal information within the statutory 40 days;
- The right to prevent processing in certain circumstances; and,
- The right to correct, rectify, block or erase information regarded as wrong information.

[1] Data Protection Act, 1998 (http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_2#pt1-l1g1)

### 6.4 How will Redditch Borough Council Ensure Compliance?

In order to ensure it meets its obligations under the Data Protection Act, Redditch Borough Council will ensure that:

- There is an individual with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Persons wishing to make enquiries about handling personal information, whether a member of staff or a member of the public, is aware of how to make such an enquiry.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.

Redditch Borough Council will, through appropriate management and the use of strict criteria and controls,:

- Observe fully conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of Data Subjects can be fully exercised under the Data Protection Act.

### 6.5 What Roles and Responsibilities have been Assigned?

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are as follows :-

#### 6.5.1 Information Manager

The Information Manager will promote this policy and provide detailed advice training and resources to departments to facilitate the correct processing of Requests for Access and other Data Protection related issues and will also monitor departments to ensure compliance with statutory and regulatory obligations.

#### 6.5.2 Senior Management

Senior management will provide support and approval for this Data Protection Policy and any related initiatives across the Council. It will also ensure that adequate funding is made available.

#### 6.5.3 Information Management Group

Members of the Information Management Group will meet regularly to review information management across the Council. As part of this they will address any Data Protection related issues that arise and generate initiatives or communications as necessary to ensure compliance with Redditch Borough Council policy.

### 6.5.4 Departmental Managers

Departmental managers are responsible for ensuring that Redditch Borough Council Data Protection Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing or funding are communicated back to their strategic directors in a timely manner.

### 6.5.5 Individual Employees

Individual employees will be responsible for understanding this Data Protection Policy and ensuring that Requests for Access and other Data Protection related issues in their own department are handled in compliance with this policy.

## 6.6 Freedom of Information Act

The Freedom of Information Act came into force in January 2005. By granting a general right of access to records held by Public Authorities it encourages an attitude of openness and will enable the public to scrutinise their decisions and working practises. The key features of the Freedom of Information Act are:

- Every Council employee has a duty to provide advice and assistance to anyone requesting information.
- The public has a general right of access to all recorded information held by the Council and some Independent Contractors. Subject to exemptions set out in the Freedom of Information Act, a requester has the right to know whether a record exists and the right to a copy of that record supplied in a format of their choice.
- Every Council must adopt and maintain a Publication Scheme, listing what kinds of record it chooses to publish, how to obtain them and whether there is a charge involved.

The Information Commissioner’s Office will oversee the implementation and compliance with the Freedom of Information Act and the Data Protection Act 1998.

## 6.7 Individual Responsibilities

All Councillors must accept responsibility for maintaining Information Security standards within the Council.

All managers must accept responsibility for initiating, implementing and maintaining security standards within the Council.

All non-managerial users must accept responsibility for maintaining standards by conforming to those controls, which are applicable to them.

ICT will be responsible for implementation of the controls marked for IT specialists.

Local managers must undertake yearly assessments of security risks within their own areas to ensure that the security breaches are kept to a minimum.

## 7 Policy Compliance

If any user is found to have breached this policy, they will 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.

## 8 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 |

## 9 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 Information Manager.

## 10 References

Internal guidance on implementation of the Data Protection Act, and key Data Protection Act related documents are available to Council employees via the Redditch Borough Council Intranet:

General guidance and a free helpdesk dealing with Data Protection Act related issues are available to Council employees and the public via the Internet on the Information Commissioner's website at:

http://www.ico.gov.uk/

The Data Protection Act can be accessed on the Internet via the UK Statute Law Database at:

http://www.statutelaw.gov.uk/Home.aspx

The following Redditch Borough Council policy documents are relevant to this policy, and are referenced within this document:

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

## 11 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.

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# Policy Document

# Remote Working Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Email Policy |
| **Author** | Mark Hanwell |
| **Filename** | Remote Working. doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Email Policy |
| **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 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.

## 2 Purpose

The purpose of this document is to state the Remote Working policy of Redditch Borough Council.

Portable computing devices are provided to assist users to conduct official Council business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

## 3 Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who use Redditch Borough Council IT facilities and equipment remotely, or who require remote access to Redditch Borough Council Information Systems or information.

## 4 Definition

This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of Redditch Borough Council IT equipment and personal IT equipment when working on official Council business away from Redditch Borough Council premises (i.e. working remotely).

This policy also applies to all users' use of Redditch Borough Council IT equipment and personal IT equipment to access Council information systems or information whilst outside the United Kingdom.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Tablet PCs.
- PDAs.
- Palm pilots.
- Mobile phones.
- Text pagers.
- Wireless technologies.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. The mobility, technology and information that make portable computing devices so useful to employees and organisations also make them valuable prizes for thieves. Securing PROTECT or RESTRICTED data when users work remotely or beyond the Council network is a pressing issue – particularly in relation to the Council's need as an organisation to protect data in line with the requirements of the Data Protection Act 1998 (see the Legal Responsibilities Policy]).

This policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to PROTECT and RESTRICTED information.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

All IT equipment (including portable computer devices) supplied to users is the property of Redditch Borough Council. It must be returned upon the request of Redditch Borough Council. Access for ICT Services staff of Redditch Borough Council shall be given to allow essential maintenance security work or removal, upon request.

All IT equipment will be supplied and installed by Redditch Borough Council ICT Service staff . Hardware and software **must only** be provided or authorized by Redditch Borough Council.

Where users access Government Connect Secure Extranet (GCSx) type services, facilities or RESTRICTED information, **under no circumstances** should non-Council owned equipment be used.

### 6.1 User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site.

- Users will not install or update any software on to a Council owned portable computer device.

- Users will not install any screen savers on to a Council owned portable computer device.

- Users will not change the configuration of any Council owned portable computer device.

- Users will not install any hardware to or inside any Council owned portable computer device, unless authorised by Redditch Borough Council ICT department.

- Users will allow the installation and maintenance of Redditch Borough Council installed Anti Virus updates immediately.

- Users will inform the ICT Helpdesk of any Council owned portable computer device message relating to configuration changes.

- All faults must be reported to the ICT Helpdesk.
- Users must not remove or deface any asset registration number.
- User registration must be requested from the ICT helpdesk. Users must state which applications they require access to.
- The IT equipment may not be used for personal use by staff. Only software supplied and approved by Redditch Borough Council can be used (e.g. Word, Excel, Adobe, etc.).
- No family members may use the IT equipment. The IT equipment is supplied for the staff members' sole use.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Redditch Borough Council may recover the costs of repair.
- The user should seek advice from Redditch Borough Council before taking any Council supplied ICT equipment outside the United Kingdom. The equipment may not be covered by the Council's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel.
- Redditch Borough Council may at any time, and without notice, request a software and hardware audit, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any information on that device. Any data being removed from the council network should be done so using an encrypted BDC memory stick. For further information, please refer to the Email Policy.
- Any user accessing GCSx type services or facilities, or using GCSx PROTECT or RESTRICTED information, must only use Council-owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely.

### 6.2 Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use.

Users must ensure that access / authentication tokens and personal identification numbers are kept in a separate location to the portable computer device at all times. All removable media devices and paper documentation must also not be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing PROTECT or RESTRICTED information must be disposed of in the 'confidential waste' bins.

### 6.3 Access Controls

It is essential that access to all PROTECT or RESTRICTED information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all PROTECT or RESTRICTED data held on the portable device must be encrypted.

Dual-factor authentication must be used when accessing the Council network and information systems (including Outlook Web Access) remotely via both Council owned and non-Council owned equipment.

Access to the Internet from Redditch Borough Council owned ICT equipment, should only be allowed via onward connection to Council provided Proxy Servers and not directly to the Internet.

### 6.4 Anti Virus Protection

ICT will deploy an up-to-date Anti Virus signature file to all users who work away from the Redditch Borough Council premises. Users who work remotely must ensure that their portable computer devices are connected to the corporate network at least once every two weeks to enable the Anti Virus software to be updated.

### 6.5 User Awareness

All users must comply with appropriate codes and policies associated with the use of IT equipment. This includes the following.

- Email Policy.
- Internet Acceptable Use Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- IT Access Policy.

It is the users' responsibility to ensure their awareness of and compliance with these.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to PROTECT or RESTRICTED information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as Redditch Borough Council itself.

## 7 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..

## 8 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 |

## 9 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.

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document.

- Email Policy.
- Internet Acceptable Use Policy.
- Software Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- IT Access Policy.
- Legal Responsibilities Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.

- IT Infrastructure Policy.
- Communications and Operation Management Policy.

## 11 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.

REDDITCH BOROUGH COUNCIL

making a difference

www.redditchbc.gov.uk

# Policy Document

# Removable Media Policy

[23/08/2011]

## Document Control

| |
|---|
| Redditch Borough Council |
| Removable Media Policy |
| Mark Hanwell |
| Removable Media Policy.doc |
| Mark Hanwell – ICT Transformation Manager |
| [Communications and Operation Management Policy |
| [Marking Classification] |
| 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 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.

## 2 Purpose

This document states the Removable Media policy for Redditch Borough Council. The policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of Redditch Borough Council's computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

## 3 Scope

This policy applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Redditch Borough Council information, information systems or IT equipment and intends to store any information on removable media devices.

## 4 Definition

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Council to conduct official business on removable media devices.

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. Information is used throughout the Council and sometimes shared with external organisations and applicants. Securing PROTECT or RESTRICTED data is of paramount importance – particularly in relation to the Council's need to protect data in line with the requirements of the Data Protection Act 1998. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Council. It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Council's needs.

This policy aims to mitigate the following risks:

- Disclosure of PROTECT and RESTRICTED information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

## 6 Applying the Policy

### 6.1 Restricted Access to Removable Media

It is Redditch Borough Council's policy to prohibit the use of all removable media devices except those that are pre-authorised. The use of removable media devices will only be approved if a valid business case for its use is developed. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the ICT Helpdesk. Approval for their use must be given by your line manager.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

### 6.2 Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased. Non-council owned removable media devices **must not** be used to store any information used to conduct official Council business, and **must not** be used with any Council owned or leased IT equipment.

The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by the Council and approved by the ICT Manager or has been sanctioned for use by the ICT Manager.

### 6.3 Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for Council purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system. For further information please see Remote Working Policy and Communications and Operation Management Policy].

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must be encrypted.

Users should be aware that the Council will audit / log the transfer of data files to and from all removable media devices and Council-owned IT equipment.

### 6.4 Incident Management

It is the duty of all users, including Council Members, to immediately report any actual or suspected breaches in information security to the ICT Helpdesk.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the ICT helpdesk.

### 6.5 Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the ICT helpdesk should removable media be damaged.

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.

### 6.6 Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be returned to ICT for disposal.

## 7 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 ICT Helpdesk

## 8 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, councillors, all temporary staff, all contractors etc |

## 9 Review and Revision

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

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document.

- Legal Responsibilities Policy.
- Remote Working Policy.
- Information Security Incident Management Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy.

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

## 11 Key Messages

- It is Redditch Borough Council's policy to prohibit the use of all removable media devices except those pre-authorised by ICT. 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 ICT **must not** be used.
- Damaged or faulty removable media devices must be returned to ICT.
- 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.

REDDITCH BOROUGH COUNCIL
making a difference
www.redditchbc.gov.uk

# Policy Document

# Software Policy

[23/08/2011]

## Document Control

| | |
|---|---|
| **Organisation** | Redditch Borough Council |
| **Title** | Software Policy |
| **Author** | Mark Hanwell |
| **Filename** | Software Policy.doc |
| **Owner** | Mark Hanwell – ICT Transformation Manager |
| **Subject** | Software Policy |
| **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 Policy Statement

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

## 2 Purpose

The purpose of this document is to state the software policy of Redditch Borough Council.

All existing Council policies apply to your conduct with regard to software, especially (but not limited to) the following:

- Email Policy.
- Internet Acceptable Usage Policy.
- IT Access Policy.
- Remote Working Policy.

## 3 Scope

This document applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Redditch Borough Council purposes.

## 4 Definition

This policy should be applied at all times that the Council's computer equipment or Information Systems are used.

## 5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

## 6 Applying the Policy

### 6.1 Software Acquisition

All software acquired by Redditch Borough Council must be purchased through the ICT Department. Software acquisition channels are restricted to ensure that Redditch Borough Council has a complete record of all software that has been purchased for Redditch Borough Council computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a Council machine as there is a serious risk of introducing a virus.

### 6.2 Software Registration

The Council uses software in all aspects of its business to support the work carried out by its employees. In all instances 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.

Software must be registered in the name of Redditch Borough Council and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The ICT department maintains a register of all Redditch Borough Council software and will keep a library of software licenses.

Redditch Borough Council holds licences for the use of a variety of software products on all Council Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer.

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

### 6.3 Software Installation

Software must only be installed by the ICT department once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by ICT.

Software may not be used unless approved by the ICT Transformation Manager or their nominated representative.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may download or install any free or evaluation software onto the Council’s systems without prior approval from ICT.

### 6.4 Personal Computer Equipment

Redditch Borough Council computers are Council-owned assets and must be kept both software legal and virus free. Only software acquired through the procedures outlined above may be used on Redditch Borough Council machines. Users are not permitted to bring software from home (or any other external source) and load it onto Redditch Borough Council computers. Council-owned software cannot be taken home and loaded on a user's home computer.

### 6.5 Software Misuse

Redditch Borough Council will ensure that Personal Firewalls are installed where appropriate. Users **must not** attempt to disable or reconfigure the Personal Firewall software.

It is the responsibility of all Council staff to report any known software misuse to their line manager. Councillors should inform the ICT Transformation Manager of such instances.

According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any Redditch Borough Council user who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under the circumstances. Redditch Borough Council does not condone the illegal duplication of software and will not tolerate it.

## 7 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 ICT.

## 8 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 |

## 9 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.

## 10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- IT Access Policy.
- Remote Working Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

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

## 11 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 e.g. ipod, mobile phone, personal memory stick, email) 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.