



# Policy Document

# Remote Working Policy

[23/08/2011]

## Remote Working Policy

---

### Document Control

<b>Organisation</b>	Redditch Borough Council
<b>Title</b>	Email Policy
<b>Author</b>	Mark Hanwell
<b>Filename</b>	Remote Working. doc
<b>Owner</b>	Mark Hanwell – ICT Transformation Manager
<b>Subject</b>	Email Policy
<b>Protective Marking</b>	Unclassified
<b>Review date</b>	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	23 <sup>rd</sup> August 2011

### Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

**Contents**

1	Policy Statement	4
2	Purpose	4
3	Scope	4
4	Definition	4
5	Risks	4
6	Applying the Policy	5
6.1	User Responsibility	5
6.2	Remote and Mobile Working Arrangements	6
6.3	Access Controls	7
6.4	Anti Virus Protection	7
6.5	User Awareness	7
7	Policy Compliance	7
8	Policy Governance	8
9	Review and Revision	8
10	References	8
11	Key Messages	9

## 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.

<b>Responsible</b>	ICT Transformation Manager
<b>Accountable</b>	Head of Business Transformation
<b>Consulted</b>	Corporate Management Team
<b>Informed</b>	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.