ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

SECURITY POLICY

REMOTE WORKING

Introduction

This policy defines the security rules and responsibilities that apply when doing council work outside of council offices at any time (also known as remote working). Its aim is to protect residents, service users, and the council. The policy applies to every type of remote working, covering both the remote use of electronic devices and paper documents.

Policy Statement

The council will provide training or communications and ensure everyone working on council business from outside of council offices is aware of their responsibilities.

Remote workers must comply with the policy and complete any required security training so that they are equipped to work outside of council offices in a secure manner in compliance with the UK Data Protection Act.

The council may at any time, and without notice, request a software and hardware audit, and ask permission to have access to, or remove, any council owned electronic equipment used for remote working.

Not covered by the Policy

Additional security measures needed when remotely accessing the Government IT Network are not included in this policy. They are described in the Remote Working Access to Government Data Policy.

Those Affected by the Policy

This policy applies to Councillors, employees of the council, contractors, agency workers, and others working in a similar capacity. It applies to volunteers and partner organisations or individuals who have a need to access council information.

The policy does not cover work done by external consultants who independently use their own IT technology and information assets. Their Data Protection Act and information protection obligations must be stated in their council work contract.

Roles and Responsibilities

1. Directors, Heads of Service, Service Leads and Managers – Approve requests for remote working, and ensure staff are trained and aware of the policy rules.

2. Remote Workers are responsible for:
   (a) submitting requests to their council manager to authorise remote working and the use of IT facilities and information,
   (b) their compliance with the policy, and
   (c) providing access to council equipment or information requested by the council or its agents after a security breach or concern.

3. The council IT Service is responsible for:
   (a) providing secure remote working hardware and software
   (b) providing remote IT network connection technology, and
   (c) providing advice, IT support, and monitoring compliance.

This may be delegated to an approved IT support service.

Policy Compliance
If you are found to have breached this policy by not complying with its rules and responsibilities you may be subject to the council's disciplinary procedure or other action. If you are suspected of breaking the Law, you may be subject to prosecution.

If you do not understand the policy or how it applies to you, seek advice from your council manager or from the Information Governance Team.

Applying the Policy
This section explains remote working responsibilities and the rules that apply.

<u>Authorisation</u>
Rule 1 Obtain management authorisation before working outside of council offices. Get permission to utilise any electronic equipment, software or documents.

<u>Physical Security</u>
Rule 2 Do not take documents out of the office unless they will actually be used. Before taking legal documents out get approval from your council manager.

Rule 3 Be vigilant and protect council equipment and documents when walking, when travelling on public transport, or by any other means of transport.

Rule 4 Make sure your council portable computer is kept separate from other council documents, notebooks, USB memory sticks, or mobile phones when working remotely.

Rule 5 Make sure that physical security tokens and portable computer media are kept physically separate from related computer equipment at all times.

Rule 6 Protect council IT equipment and documents outside of council offices. When not in use they must be kept out of sight, or locked away if possible.

Rule 7 When staying in hotels or other accommodation keep council IT equipment, computer media or paper-based information protected. Use complimentary hotel security facilities if available.

Rule 8 Any theft or loss of equipment or information must be reported to:

(a) The police if theft is suspected, and a crime reference Number obtained. n
(b) The council's phone provider 24x7 emergency number if a phone is involved.
(c) The council manager responsible.
(d) The IT Service Desk if equipment needs to be de-activated.
(e) The Information Governance Team by submitting a security incident.

Other precautions can help to reduce the risk of theft or unauthorised access. These are offered as guidance, but are not mandatory. If council services decide to adopt any of them they must provide appropriate support for their staff and other workers.

(i) Keep bags used to carry equipment or documents locked when out of the office. A small suitcase lock is sufficient.
(ii) Disguise laptops by using ordinary bags rather than laptop bags or briefcases.
(iii) If possible store council equipment and information upstairs when not at home.

(iv) When you leave your home keep council electronic equipment and documents out of sight and not visible through windows or doors.

Unauthorised Access

Remote workers are responsible for preventing unauthorised access to council equipment or information, whether electronically or on paper.

Rule 9 No family members or other unauthorised persons may be given access to council IT equipment, information or documents.

Remote Storage of Data and Use of Email

Rule 10 Council data must be stored on the council IT network or facilities unless there is no alternative. Management authorisation must be obtained before any data is stored externally, e.g. stored on the Internet, on a portable electronic device, on a computer disk drive, or on portable computer media.

Rule 11 Council data must not be emailed to an external personal or business email address, unless there are exceptional circumstances.

The IT Service must authorise any exceptional circumstances arising from rules 10 and 11.

Rule 12 Personal or sensitive personal data stored on a computer disk drive outside the council IT network or facilities must be encrypted and access protected by a strong password.

Remote Use of Paper

Rule 13 Do not print information outside council offices unless absolutely necessary. Do not leave printed council information where it can be read by others.

Rule 14 Paper documents containing personal or sensitive data must be disposed of by either (a) using a cross-cut shredder, or (b) returning them to the office and using the council's confidential waste paper disposal service.

Remote Access to IT Equipment

Remote workers must accept responsibility for use of any email accounts used to conduct council business, and for any other access made to council IT services.

Rule 15 Protect your council logon user identifiers, passwords, access tokens, or other access mechanisms. Never share or disclose your council user identifier and password with anyone else. Never use anyone else's user identifier and password to gain access to council IT facilities.

Rule 16 Switch off or log off any IT equipment used remotely when it is not in use or left unattended.

Technical Security

Rule 17 Remote IT equipment must be connected to the council IT network or facilities by an approved technical connection. The options are:

(a) through a dedicated council broadband line
(b) through a mobile telephone connection operating on council IT equipment
(c) through a Virtual Private Network link
(d) by using a non-council computer through an encrypted Internet link into the

council IT network or facilities. Non-council computers may only be used if protected by reputable anti-virus software receiving regular anti-virus definition updates. Reputable anti-virus software can be obtained free of charge.

It is permissible to use an existing home broadband link to access the council IT network if it is set up securely (see the guidance in the council's Use of Wireless Communications Security Policy).

Rule 18 Access to the Internet from council owned IT equipment should only be allowed via the council IT network or facilities, and not directly.

Rule 19 Remote workers must not install or update any hardware, software or make other changes to council computers and electronic equipment. These changes must be carried out by the IT Service or authorised support staff.

Rule 20 Council IT equipment should be connected to the IT network or Internet regularly to ensure the latest anti-virus definitions are obtained.

Rule 21 Remote workers are responsible for the technical protection of the computers they use for council business. This includes, but is not limited to, the acceptance of regular operating system patches, other software security updates, and receipt of regular anti-virus definition updates.

Rule 22 If you suspect a virus infection on a council-owned computer when working remotely you must report it as soon as possible to the IT Service Desk, or to an alternative approved IT support service. You must also inform your council manager and submit a Security Incident Report. Failure to report a virus will be considered a serious breach of this policy.

Remote Working outside of the UK

IT or telephony services accessed from outside the United Kingdom (including Internet access) have significantly higher security risks.

Rule 23 Written authorisation must be obtained from a Director or Head of Service before taking council portable electronic devices outside the UK.

Rule 24 Council personal or sensitive personal data must not be accessed through IT or telephony services from outside the United Kingdom.

Policy Training

Online policy training and knowledge testing will be offered whenever possible.

Related Policies and Procedures

Government GCSx IT Acceptable Usage Policy
Health, Safety and Lone Working Guidance documents
Remote Working Access to Government Data Policy
Security Incident Reporting Policy
Storage of Information Policy
Supplier and Third Party IT Acceptable Usage Policy
Use of Wireless Communications Policy

Related Legal and Regulatory Obligations

UK Data Protection Act
Information Security Management Standard ISO/IEC 27001:2005

Definitions

Personal or Sensitive Information - Personal data is data relating to a living, identifiable individual. Sensitive data includes personal data and also any other data that may cause financial loss, distress, or reputation damage.

Portable Electronic Device (PED) – any piece of equipment that is portable and stored electronic data. This includes, but is not limited to laptops, tablet computers, handheld computers, cameras, Internet smart phone, and mobile phones.

Encrypted data – data that is ‘scrambled’ by software using a mathematical formula to prevent it from being read by unauthorised persons.