ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk

Royal Borough
of Windsor &
Maidenhead

Security Policy

RECEIPT OF EXTERNAL DATA ON PORTABLE COMPUTER MEDIA

Introduction

The council's work often requires exchanges of information with external organisations or the public. This policy covers the security of data received by the council. This includes information from members of the public; other organisations; and from central government.

Policy Statement

Use of all external data received on portable computer media must be authorised by management, and security checked against the most recent anti-virus and malware definitions available from the council's virus and spyware checking software.

Failure to virus check a USB memory stick, CD/DVD or other portable computer media will lead to disciplinary or other action if as a result a serious virus infection occurs.

Policy Aim and Benefits

The policy will help to protect the council, its staff, other organisations, and the public from potential damage caused by external data. The benefit will be a reduced risk of damage to the council caused by infected external data.

Not covered by this Policy

The policy does not cover paper-based information.
It also does not cover the reading of portable computer media on public workstations in libraries and other public areas. These workstations must be isolated and separated from the council's secure IT network.
It does not cover external information sent to the council using e-mail.

Those Affected

This policy applies to any person using the RBWM secure IT network who is in receipt of external electronic data from other organisations or the public.

Roles and Responsibilities

1. Users of council IT facilities – must ensure that external data received on portable computer media is electronically checked against the latest anti-virus and malware definitions.
2. IT Service – will oversee electronically checking of portable computer media against the latest anti-virus and malware definitions.
3. IT Service – responsible for ensuring the latest virus and spyware software is loaded to allow the most secure checking of external data.

Policy Compliance

This policy must be complied with. Any breach of the policy could constitute a disciplinary offence. If you do not understand the implications of this policy, or how it affects you, seek advice from your line manager, the IT Service, or the Information Governance team.

Security Checking Procedure
The procedure steps are outlined below.

Users of council IT facilities
1. Obtain management authorisation before storing any external data (provided on portable computer media or devices) on the RBWM IT network.

2. Get all external portable computer media thoroughly virus checked.
This includes CDs, DVDs, USB memory sticks, memory cards, digital camera and mobile telephone memory, or other portable media

The security check can be done by logging a call to the IT Service Desk to request an external data security check, specifying the medium and data involved, and any business deadlines.

3. If the security check is done by the IT Service on a separate computer they will:
   a) Confirm when the data will be checked.
   b) Complete the security check and store the data in an agreed location.

Related Policies and Documents
Storage of Information Policy

Related Legal and Regulatory Obligations
UK Data Protection Act