ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk

Royal Borough
of Windsor &
Maidenhead

SECURITY POLICY

STORAGE OF INFORMATION

Introduction and Policy Aim

When doing work for the council all data and information must be stored securely.
The risk of loss, theft, or unauthorised disclosure is significantly higher when electronic data is stored outside of the council's IT network or facilities.

Policy Statement

Council electronic data should be stored on the council IT network or facilities whenever possible because it provides the strongest level of protection.

The storage of council data onto portable electronic devices or portable computer media is only permitted if using council IT equipment or computer media. This type of storage outside the IT network must be authorised by a council manager.

Storage of council data on non-council business or privately owned computers has a significantly higher risk. This storage requires approval from the council senior manager responsible and must be registered with the Information Governance team.

Storage of council data on the Internet, or elsewhere, also has a higher risk and requires a business justification. This higher risk storage must be authorised by a senior manager, and registered with the Information Governance team.

Council personal data stored outside the council IT network or facilities must be sufficiently protected against unauthorised access, e.g. by using data encryption.

Sensitive or personal paper information (documents) must be locked away when not in use. Information should only be stored on paper if there is an operational or statutory reason, and must be disposed of securely when there is no further need to use it.

Not covered by this Policy

Access to the council Internet portals using non-council IT equipment.

Those Covered by the Policy

Councillors, employees of the council, contractors, agency staff, and others working in a similar capacity are covered. The policy also applies to partner organisations or others who have a need to utilise council data and information.
Work done by external consultants who independently use their own IT technology and information stores is not covered. Their Data Protection Act and specific information protection obligations must be stated in their council contract of work.

Roles and Responsibilities

1. Councillors, employees and anyone else conducting business on behalf of the council – must obtain management approval before storing information outside the council IT network or facilities. This includes the physical storage onto portable computer media or portable electronic devices, storage on computers, or Internet data storage.
2. Council Directors, Heads of Service and Managers – must ensure Councillors, employees and others under their supervision have obtained approval for all

storage of information outside of the council IT network or facilities.

3. The IT Service – is responsible for
(a) procuring and supporting computer hardware and software, including software for reading or writing CDs and DVDs; setting up encryption on devices.
(b) updating the asset registers used for portable electronic equipment
(c) enabling USB port access to PEDs and CD/DVD writing.

The IT Service may delegate these services to approved IT support providers.

4. The Information Governance team – is responsible for the registration of storage of data outside the Council IT network, and for compliance/risk monitoring.

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

Management authorisation must be obtained before storing data outside of the council IT network or facilities. The authorisation options are as follows:

Registration of Data Storage onto Portable Electronic Devices or Computer Media

This includes, but is not limited to, data storage on laptops, portable computers, tablets, USB memory sticks, CD/DVD writing, cameras, dictaphones, portable hard disk drives, and memory cards. Storage of data in these ways must be registered using the Registration of Data Storage onto Portable Electronic Devices or Computer Media form.

Other Data Storage Outside the Council IT Network or Facilities

Permission to store council data outside the council IT network or facilities must be sought by the person who will store the data. A Request to Store Data Outside the Council IT Network form must be submitted. The Information Governance team will register the request and may take action if the request exposes the council to unacceptably high risk.

Ordering Portable Electronic Devices

Council managers must order portable electronic devices, or software to read or write CDs or DVDs, from the IT Service using the ICT Order Form. The name of the person(s) who will use the electronic device or read/write CDs or DVDs must be confirmed when the order is placed. They must accept the security conditions of use.

Transfer of Ownership

The transfer of a portable electronic device from one person to another must be registered by submitting the Registration of Data Storage onto Portable Electronic Devices or Computer Media Form.

Related Policies and Documents

Supplier and Third Party Acceptable Usage Policy (incl. conditions of use 6,9,14,15)
Information Retention and Disposal Policy   Information Asset Management Policy

Related Legal and Regulatory Obligations

UK Data Protection Act

Definitions

Disk drive – part of a computer where data can be stored, known as a local disk drive.
Personal data - information is data relating to a living, identifiable individual.
Sensitive data – any data that might cause financial loss, distress, or damage to reputation. Personal data may be sensitive or highly sensitive.
Portable Electronic Equipment/Device (PED) - any portable piece of equipment that has the ability to store, process or transmit information. Examples include (but are not limited to) laptops, tablets, Internet smartphones, cameras, and dictaphones.
Computer Storage – any electronic medium used to store data.
Internet Data Store – a place where data is stored on the Internet
Data Encryption – The 'scrambling' of information by software using a mathematical formula to prevent it from being understood by anyone not authorised to read it.