ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk

Royal Borough
of Windsor &
Maidenhead

SECURITY POLICY

INFORMATION HANDLING

Introduction and Policy Aim

The Royal Borough of Windsor and Maidenhead (the council) recognises the need to protect council owned information and electronic devices. This policy defines the rules and responsibilities needed for the secure handling and protection of council information. The aim is to establish professional good practice.

The council's Remote Working Security Policy should be read alongside this policy. The two policies provide a comprehensive statement of the actions needed to protect council information and electronic devices.

Policy Statement

All council paper information and electronic data must be protected appropriately. If it is personal or sensitive personal data it must be protected in line with the UK Data Protection Act. Sensitive, non-personal, data must also be protected.

The council is committed to provide security training and communications to ensure everyone working for the council has the opportunity to understand their responsibilities. The stated preference is for online training and knowledge tests.

All council workers must complete the required security training and handle council information and electronic equipment in a secure manner.

Not Covered by this Policy

The classification of electronic data stored on the council IT network or facilities.

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 UK Data Protection Act and information protection obligations must be stated in their council work contract.

Roles and Responsibilities

1. Councillors, employees and others conducting council business – must comply with this policy whenever they handle council information on paper, electronically, or verbally. They must also complete any related training requested by the council.

2. Council Directors, Heads of Service, Service Leads and Managers – have overall responsibility for the protection of council electronic devices, documents, and information. They must ensure employees and others working for them have sufficient opportunity to understand this policy, its rules and related procedures.

They have the authority to implement local policies and procedures as long as they are consistent with this policy.

3. The Council IT Service – is responsible for the provision of technology solutions and services that enable secure electronic information handling.

4. The Information Governance Team – is responsible for providing information security training and communications, and for policy compliance 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

The policy rules are defined below. You must also comply with published council information handling procedures that are used to protect information.

Proving Identity

Rule 1 The council must provide employees and others doing work for the council with an identity badge. It must be worn at all times whilst on council premises or when doing work for the council.

Rule 2 The identity of any person being contacted by, or contacting, the council must be checked and proven before sensitive or personal information is provided to them verbally, on paper or electronically.

Level of Information Protection Required

Council information and data must be appropriately protected.

The council's Protective Marking security policy applies to authorised users of the Government IT network, who are responsible for the safekeeping of information sent to or received from GCSx email partners and central government.

Rule 3 Government GCSx emails that contain sensitive or personal data must be given a security protective marking to define the protection needed against loss, theft or unauthorised access.

Protecting Voice Information

Precautions must be taken to protect sensitive or sensitive personal data shared in conversation so that it cannot be accidentally overheard.

Rule 4 Take precautions to ensure that conversations about sensitive or personal council matters cannot be overheard. These conversations should not be held in public places when members of the public may overhear.

Rule 5 After listening to voice recordings in the course of council business, you must not disclose what you have heard to unauthorised person(s).

Sending, Receiving or Storing Paper Documents

Use of Post

All post received or sent by the council must be handled in a secure manner using defined post handling procedures. The specific policy rules for use of post are:

Rule 6 Any post received by the council with an ‘only to be opened by addressee’ marking (or similar wording) must only be opened by that addressee.

Rule 7 All letters sent either internally or externally that contain sensitive personal data must be in an envelope and protected with the following marking: ‘Private and Confidential’. These words may also be used for letters containing commercial or other types of non-personal sensitive information.

Rule 8 A ‘return to sender’ name and address must be written on envelopes or packages sent in case the post is not correctly delivered. For post containing sensitive personal data a named council worker or council service area must be included in the return to sender details.

Rule 9 Additional protection must be considered (e.g. collection from a council office, or hand delivery to the service user’s home address) when information being sent includes sensitive personal data, and serious damage could be caused if it were mis-directed or lost.

Delivering of Documents to Service Users

Rule 10 Council documents or letters delivered by hand to service user homes must only be given to a named addressee, whose identity must be checked before the document or letter is handed over. These documents or letters must comply with rules 7 and 8 above.

Rule 11 When a service user picks up a document or letter at council offices, their identity must be checked before they are given it.

For rules 10 and 11 above a receipt must be signed to provide evidence that the service user has received the document or letter.

Printing, Photocopying, Use of FAX and Scanning Documents

Only use FAX transmissions if there is no other alternative.

Rule 12 You must prevent unauthorised access to personal or sensitive personal information you print, copy, FAX or scan, by complying with the published information handling security procedures.

Storage of Paper Documents

Rule 13 Personal or sensitive documents must be kept out of sight when not in use, and must be locked away overnight when kept in council offices. The council will provide suitable secure storage, e.g. lockers, cabinets or safes.

Rule 14 The content of council safes must be recorded, and this record must be kept separately away from the safe. The names of staff issued with safe keys must be recorded. If keys are lost or stolen then the lock must be changed.

Destruction of Paper Documents and Information

Rule 15 Personal or sensitive personal documents must be disposed of by using the council confidential waste service, or by cross-cut shredding. Electronic devices must be destroyed using the IT Service destruction service.

Use of Electronic Storage Devices, Documents, Data and Emails

Keeping Information Out of Sight

Rule 16 Ensure information displayed on your computer screen is protected when you leave your computer unattended. Lock your computer by logging out or by pressing 'control-alt-delete' simultaneously then press the enter/space key.

Take precautions to avoid your on-screen emails, documents or data being overseen accidentally or deliberately by unauthorised person(s).

Sending or Receiving Email

Sending Email

Your risk of error increases when you work under pressure. A good way to reduce your risk is to 'pause and re-check' before you send an email.
The rules below apply when sending emails on behalf of the council.

Rule 17 Redact personal data about service users, e.g. replace names by initials or computer reference numbers. If your email forwards a string of previous emails check their content as well. Remove or redact earlier data if required.

Rule 18 Use email distribution lists carefully. Make certain that everyone in the list is authorised to read the information you send.

Rule 19 When you create an external distribution list containing external personal email addresses get it double-checked before starting to use it.

Rule 20 Use the blind copy option when you are creating an email to send externally to more than one private email address. This is because unauthorised disclosure of private email addresses breaches the UK Data Protection Act.

Rule 21 Do not use your private email address to send or receive council emails.

Rule 22 Protect personal or sensitive personal data you send externally over the Internet. Data encryption is recommended by the Information Commissioner and is the safest alternative.

GCSx email provides this level of protection. If GCSx email is not available then you must password protect sensitive or personal data by using an attachment and password protecting it.

Receiving Email

Rule 23 If you receive an email containing sensitive personal data that has been sent over the Internet without any protection, inform the sender that they have taken a risk. Request that they protect their emails in future.

Rule 24 When you reply to an email containing personal or sensitive personal data do not use 'reply to all' unless everyone copied is authorised to receive it.

Storage of Electronic Data

Rule 25 Electronic devices must be kept out of sight when not in use, and must be locked away overnight when kept in council offices. The council will provide appropriate secure storage, e.g. lockers, cabinets or safes.

Rule 26 Store data attachments received via email onto the council IT network storage areas. By doing this you reduce the risk of your email storage allocation being exceeded, and your data will be backed up.

Destruction of Electronic Storage Devices

Rule 27 Return your council electronic device to the IT Service if you no longer use it. They will check it and either safely destroy it, or re-issue it after any data left on the device has been destroyed in a secure manner.

Handling Information Remotely Outside Council Offices

Remote working covers working from home, working on the move, working in public areas, and working from the premises of another organisation.

Rule 28 Take extra precautions when working outside of council offices, as defined in the Remote Working Security Policy.

Leaving the Council

Rule 29 All council equipment and documents must be returned to the manager responsible at the end of council employment or working for the council.

Related Policies and Procedures

Information Handling Procedures Leaflets Use of Email Policy
Information Security Code of Conduct
Physical Security Policy Clear Desk Security Policy IT Access Security Policy
Remote Working Security Policy Storage of Information Policy

Legal Obligations

UK Data Protection Act

Related Documents and Sources

Information Commissioner security guidance documents

Definitions

Personal or Sensitive Data - Personal data is data relating to a living, identifiable individual. Sensitive personal data includes personal data and any other data that may cause significant harm to persons, financial loss, distress, or damage to the council's reputation.

Information - includes, but is not restricted to, verbal communication, paper documents, portable electronic devices, and council data files stored on computers.

Electronic Device – any device capable of storing electronic information and potentially requiring security protection. See examples below.

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 restricted to) laptops, tablet computers, Internet smartphones, cameras, dictaphones, memory cards.