ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

SECURITY POLICY

Use of the Internet

Introduction and Policy Aim

The Internet is one of the council's main tools for communication and information access, and there are recognised risks associated with accessing and handling information using the Internet. This policy defines your personal responsibilities and explains the protection provided when using the council's Internet facilities.

Policy Statement

Any use of Internet facilities when conducting council business must be legal, appropriate and secure.

Everyone conducting council business must comply with this policy either:
(a) when accessing council Internet facilities from any location, or;
(b) when accessing the Internet using other Internet facilities from any private business or personally owned computers and electronic equipment.

The council regards the use of its Internet facilities as being primarily for business purposes. Limited agreed personal use is permitted during working hours, and outside of normal working hours.

Not covered by this Policy

Monitoring of Internet use from non-council Internet facilities.

Those Affected by the Policy

Anyone performing council duties or providing council services using the Internet. It applies to Councillors; other organisations conducting council business; employees; contractual third parties and agents of the council.

Roles and Responsibilities

1. Users of the Internet for council business – must understand the policy and comply with it, especially the limitations on Internet use.
2. Council Managers and Team Leaders – must encourage staff to use the Internet appropriately and securely. They should ensure Internet use during work time is relevant to council business requirements, and that personal Internet use is limited.
3. The IT Service – will investigate Internet security breaches or incidents, and provide advice. The IT Service (or authorised IT support services) will set up Internet access rights for, and monitor Internet use of, council Internet facilities.

Policy Compliance

You must comply with this policy. Any policy breach could constitute a disciplinary offence or result in other council action. If a criminal offence is considered to have been committed council action may be taken to assist in the prosecution of the offender(s). If you do not understand this policy, or how it may apply to you, get advice from your council manager, the IT Service, or the Information Governance Team.

Document Title: Use of Internet Policy
Policy Owner :P M Strode
                    Page 1 of 3
UNCLASSIFIED

Date Approved: 21 November 2012
Last Updated: 20 October 2017
Next Review Date: Sept. 2018

Applying the Policy

Rule 1 - What you should use your council Internet access for
Your Internet access whilst doing work for the council may be used for the following:
(a) obtaining information or research,
(b) Council electronic commerce (e.g. purchasing council equipment);
(c) communicating with residents and members of the public;
(d) professional networking, and approved personal or professional development:
(e) appropriate and authorised use of social media networking sites.

This list is not exhaustive and other reasons may apply, but must be authorised.

Rule 2 - You are responsible for the content and security of everything you send to or receive from the Internet.
When using the Internet for council business you must identify yourself clearly.
You must not send Internet communications that hide your identity.

Internet communications are not guaranteed to be safe. Messages may be lost or intercepted. Send personal and sensitive information only to Internet sites that are protected (i.e. with an Internet address starting 'https' and with a padlock symbol shown at the bottom of the screen).

If you think your computer has a virus infection, immediately unplug your computer from any IT networks and the Internet. Any concerns, messages or warnings relating to viruses received when using council Internet facilities must be referred to the council's IT Service Desk, or to your approved IT support service.

Rule 3 - Personal use of the Internet using council Internet facilities
Personal use of council Internet facilities is normally restricted to non-work time, e.g.:
- before 8:45am;
- during lunchtimes between 12:00 and 2:30pm. and;
- after 5:15pm. on Mondays to Thursday, or after 4.45pm. on Fridays.

At the discretion of your council manager, and provided it does not interfere with your work, limited personal use of the Internet in work time is permitted.

Rule 4 - The purchase of personal goods or services is permitted using the council's Internet facilities during non-work time.

Rule 5 – Council information must not be exported to non-council Internet sites without written approval from the council manager responsible

Rule 6 – Internet access and security using council Internet facilities will be monitored
The council has a responsibility to ensure that use of its Internet facilities complies with legislation and statutory guidance.

All access is recorded, logged and may be used for the purposes of:
(a) monitoring total usage to ensure business use is not impacted by lack of capacity,
(b) monitoring access to websites and appropriate usage.

Your council computer and any data held on it are council property and may be accessed at any time by the council to ensure compliance with all its statutory, regulatory and internal policy requirements.

Document Title: Use of Internet Policy
Policy Owner: P M Strode
Page 2 of 3
UNCLASSIFIED
Date Approved: 21 November 2012
Last Updated: 20 October 2017
Next Review Date: Sept. 2018

Rule 7 – Council work conducted using private business or personally owned Internet access must comply with this security policy.

Rule 8 - You must not access specified categories of information
The consequences of accessing inappropriate Internet sites can be serious.

Except where it is strictly and necessarily required for your work (and this is agreed by management) you must **not** use your council Internet access to:
- Create, download, upload, display or access knowingly, sites that contain pornography or other material that might be deemed illegal, obscene or offensive.
- Use foul or offensive language or make defamatory or derogatory remarks.
- Represent personal opinions as those of the council, or impersonate or misrepresent others.
- Run a private business.
- Subscribe to, enter or use peer-to-peer networks or install software that allows illegal sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms.
- Subscribe to, enter or utilise online gaming or betting sites.
- Subscribe to or enter "money making" sites or use "money making" programs.

The above list is neither exclusive nor exhaustive. *"Unsuitable"* material includes data, images, audio files or video files the transmission of which is illegal under UK law.

Members of the public, and others doing council work, using council Internet facilities are protected by having access to certain categories of websites blocked.
Examples of blocked categories include but are not restricted to: illegal; pornographic; violence; hate and discrimination; and offensive web content

If you need access to any blocked categories of information using council Internet facilities, get your manager's authorisation by completing the RBWM Internet Access Request Form.

Rule 9 – You must report misuse of the Internet
If you know of any council Internet misuse that conflicts with this policy or with the Equal Opportunities policy you must report it to the council manager responsible for the work, or submit a council Security Incident Report as soon as possible.

Rule 10 – You must not download Internet software or data without checking its safety
Internet downloading is only permitted in controlled circumstances because the Internet is a primary source of virus infection. You must always check whether Internet software or data is safe to download.

If software needs to be downloaded from the Internet onto council IT equipment please submit an IT Access Request Form. Avoid infringement of copyright when downloading software. If in doubt check with the IT Service Desk or your approved IT support service.

Related Information
Social Media Policy   Use of Email Policy

Legal and Regulatory Obligations
UK Data Protection Act

Document Title: Use of Internet Policy
Policy Owner: P M Strode
Page 3 of 3

Date Approved: 21 November 2012
Last Updated: 20 October 2017
Next Review Date: Sept. 2018
UNCLASSIFIED