Internet Usage and Monitoring Policy

Contents

1. Purpose
2. Scope
3. Policy statements
4. Responsibilities
5. Internet usage principles
6. Internet monitoring
7. Monitoring principles
8. Compliance measurement
9. Sponsor
10. Custodian
11. Ensuring equality of treatment

1. Purpose

1.1 The purpose of this document is to define Carmarthenshire County Council's policy for the effective and appropriate use of the Internet.

2. Scope

2.1 Internet use refers to the use of the internet from the authority's computers and/or network.

2.2 This policy governs the Council's approach to managing the internet facilities ensuring the best interests of both the staff and the Council are upheld.

3. Policy statements

3.1 The Authority's internet facilities will be used in accordance with:

- This policy and related guidelines
- All appropriate legislation – including but not limited to the Computer Misuse Act 1990, the Data Protection Act 1998 and the Copyright, Designs and Patents Act

3.2 Internet usage will be monitored to ensure compliance with the Internet Usage Principles

3.3 This policy is approved by, and has the full support of the Council.

4. Responsibilities

4.1 The Authority will provide staff with education and training to support compliance with this policy.

4.2 All managers will be responsible for implementing the policy within their areas of responsibility.

4.3 All permanent employees, contractors and temporary staff provided with internet access will signify their acceptance of the policy and indicate their agreement to comply when they first use internet access each day.

4.4 The IT Security Officer will develop, maintain and publish procedures guidance and standards to achieve compliance with this policy

5. Internet usage principles

5.1 The use of the Authority's internet facilities indicates acceptance of the policy.

5.2 The Authority provides internet access to assist employees in the performance of their jobs. Whilst its use should be primarily for official Authority business, incidental and occasional personal use of the internet is permitted, on the understanding that:

5.3 Personal use of the internet will never impact the normal business traffic flow.

5.4 Personal use will be limited to those times outside working hours for example lunchtimes.

5.5 The Council reserves the right to filter content and block access to websites deemed unsuitable

5.6 The Council reserves the right to block downloads of files from the internet based on their type or content

5.7 No employee, consultant or contractor will attempt to access or transmit content that in any way may be interpreted as insulting, disruptive or offensive or which may be harmful to staff morale. Examples of prohibited material include but are not limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files
- Profanity, obscenity, slander, or libel
- Ethnic, religious, or racial slurs
- Any content that could be construed as harassment or disparagement of others based on their race, colour, nationality, ethnic or national origins, language, disability, religion, age, gender, gender reassignment, sexual orientation, parental status, marital status or political beliefs
- Content including articles, images, speeches or videos that promote terrorism or encourage violence**,** websites made by terrorist or extremist organisations or videos of terrorist attacks

5.8 No employee, consultant or contractor will attempt to break through any security controls whether on the Authority's systems or any other systems

5.9 No employee, consultant or contractor will attempt to download or transmit any computer virus, spyware or other malicious code using the Council's equipment or Internet link.

5.10 All internet traffic will be monitored and reviewed, and any breaches of policy may result in disciplinary action being taken

5.11 All users must ensure compliance with all relevant legislation.

5.12 All users must maintain virus awareness. Users of laptops are responsible for ensuring their virus definitions are maintained on a regular basis.

5.13 Internet use must not be for personal financial gain, for example you may not conduct your own business using the Authority's facilities.

5.14 The user logged in at a computer will be considered to be responsible for all sites visited; therefore users must remain vigilant and log off or lock their computers when away from their desks.

5.15 Users must not subscribe to email lists, which are not relevant to their job function. The volumes of messages that can be generated are high and the content may be dubious resulting in conflict with the conditions stated above.

6. Internet monitoring

6.1 The Council's internet facilities will be monitored in accordance with:-

- This policy and related guidelines
- The appropriate legislation – including the Data Protection Act 1998, the Regulation of Investigatory Powers act 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

7. Monitoring principles

7.1 The Council will automatically monitor internet access. This includes, but is not limited to, monitoring of sites visited and browsing time.

7.2 Access will be filtered according to the site categorization and content and may even be blocked entirely. Users will be notified if a site has been blocked.

7.3 Regular summary reports on internet usage will be made available to managers.

7.4 More detailed reports will be made available on request by Heads of Service.

8. Compliance measurement

8.1 Compliance with this Internet Usage and Monitoring Policy is mandatory. Breaches of this policy by staff may lead to disciplinary action being taking. Breaches by Elected Members may be reported to the Standards Committee

9. Sponsor

9.1 This Policy is owned by the Corporate Information Governance Group.

10. Custodian

10.1 It is the responsibility of the IT Security Officer to ensure that this policy is kept up to date.

11. Ensuring equality of treatment

11.1 This policy must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion, age, gender, gender reassignment, sexual orientation, parental or marital status.

If you require this document in an alternative format please contact the IT Security Officer on 01267 246326 or email **ITSecurity@Carmarthenshire.gov.uk**

Policy approved by Executive Board Member on: 14th May, 2013
Policy review date: February, 2023
Policy written by: Richard Williams CISSP