Warwick District Council

Internet Acceptable Usage Policy (Inc. Social Media)

WARWICK DISTRICT COUNCIL

www.warwickdc.gov.uk

Internet Acceptable Usage Policy (Inc. Social Media)

Revision History

Document	Internet Acceptable Usage Policy (Inc. Social Media)
Author	Ty Walter
Date Completed	10 August 2009
Reviewed Date	09 Jun 2018

Version	Revision Date	Revised By	Revisions Made
1.0	10 August 2009	Ty Walter	Original Document
1.1	20 October 2011	Ty Walter	Updated definitions,
1.2	31 May 2012	Ty Walter	Clarification of wording associated with 'Connecting to the Internet. New section added on 'Blocked Web Sites'
1.3	20 June 2013	Ty Walter	New section on monitoring Internet usage.
1.4	09 Jun 2017	Ty Walter	If the proxy server blocks a web site that is being used for personal use, it will remain blocked.
1.5	25 Aug 2017	Ty Walter	Update to the use Social Media section.
1.6	25 Jan 2018	Ty Walter	Update to Policy Statement, inclusion of Risks and copyright section. Minor amendments to the key messages.
1.7	09 June 2018	Ty Walter	Correction of a policy title – Harassment at Work corrected to Dignity at Work.
1.8	29 Jan 2019	Kris Walton	Update to the Social Media section re: Councillors

Approvals

This document requires the following approvals:

Name	Title
ICT Steering Group	
Senior Management Team	
Employment Committee	

Distribution

This document has been distributed to:

Name	Title
All Staff	
All Members	

Contents

1 Management Summary

The internet is a collection of world-wide interconnected computer systems providing access to a variety of information bases known as the World Wide Web (www).

The Internet is now firmly established as a major research, information, communication and service delivery tool within the Council but it is one with inherent security risks and without guarantees of reliability or performance.

The Council wishes to encourage the correct and proper use of the Internet, and expects staff to use this facility during the normal course of work. The Council wishes to encourage appropriate internet use by staff, and to increase their competence and understanding of its potential.

This policy determines how Council staff and members' can use the Internet professionally, ethically and lawfully without compromising citizen or staff confidentiality and whilst maintaining the security of the IT network.

The Council appreciates that it is not possible to regulate what sites are provided over the Internet, but views the content of some sites as being a risk to the confidentiality, security and integrity of Council systems and data. Therefore this policy document forms part of Warwick District Council's ICT Security and Conduct Policy and defines the acceptable use of the Internet within the Council and on council devices.

2 Policy Statement

Warwick District Council encourages the use of the Internet where it supports the aims and objectives of the Council. It is essential that the use of the Council's Internet facility complies with current legislation and does not create unnecessary business risk for the Council.

The Council will ensure that all users of its Internet facility are aware of this acceptable use policy.

3 Purpose

The objective of this Policy is to direct all users of Council Internet facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of the Internet.
- Informing users about the acceptable use of ICT facilities in relation to the internet.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the Internet.

The Internet facility is made available for the business purposes of the Council. A certain amount of personal use is permitted in accordance with the statements contained within this Policy.

It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

4 Scope

This policy is intended for all Warwick District Council Councillors, Service Areas, Partners, Employees of the Council, contractual third parties and agents of the Council who are users of the Council's Internet facilities.

Any reference in the document to "employee", "staff" or "user" is deemed to include all of these groups of authorised users.

5 Definition

This Internet Acceptable Usage Policy should be applied at all times whenever using Council devices, systems or facilities to access the Internet. This includes Council devices that have independent access to the Internet such as mobile devices (tablets) and smartphones

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This

includes online social forums such as Twitter, Facebook and LinkedIn. Social media also covers blogs, video and image-sharing websites such as YouTube and Flickr.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

6 Risks

The Council recognises that there are risks associated with the use of the Internet. This policy aims to ensure appropriate access to and use of the Council's Internet facility which will help to mitigate the following risks:

- Exposure of Council systems to malicious or harmful software.
- Hacking and other unauthorised access to council systems
- Wrongful disclosure or private, sensitive or confidential information
- Service disruption
- Exposure of the Council to vicarious liability for commitments and/or comments made by individuals.
- Damage to the Council's reputation
- Inappropriate use of resources.

7 Applying the Policy

7.1 Internet Monitoring

The Council is ultimately responsible for all business communications but will, as far as possible and appropriate, respect your privacy while you work. It is important, however, that you understand that the Council will monitor the use of all of its ICT Equipment, including the use of the Internet.

You should be aware that this monitoring may reveal personal information about you, for instance which websites you visit etc.

All users should be aware that Internet usage is monitored electronically and recorded centrally. These arrangements will be applied to all users and may include but are not be limited to checking content, logging Internet activity, and denying transmission. All monitoring will be undertaken in accordance with the Council's Monitoring Policy (Electronic Communications). The policy also describes the reasons for monitoring electronic communications

Information recorded by the automated monitoring systems can be used to identify an individual user and show, for example, a website or document that a user has been viewing.

Because of this, **staff must not assume privacy** in their use of the Council's systems, even when accessing the systems in their personal time, such as during lunchtime. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By

carrying out such activities using Council facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

This software is also used to prevent Internet misuse, for example, by blocking access to inappropriate sites or materials by using filtering software. The software blocks access to sites which are classified using standardised criteria to protect staff and the organisation from inappropriate material and sites.

In order to monitor Internet access, a series of routine reports have been established. On a weekly basis a report is generated which shows the staff members attempting to access adult/sexually explicit sites

Other areas can be monitored if necessary for legitimate business reasons.

These reports are specifically aimed at identifying users who may be repeatedly trying to access inappropriate sites or who may be using the Internet excessively during work time.

7.2 Personal Use

All Warwick District Council employees are entitled to access the Internet for personal use during non-working time, for example during the lunch hour or during official breaks. However, when using the Internet the following should be adhered to:

- Employees may use the Internet to purchase personal items such as books, cameras, holidays, etc. However, the Council accepts no responsibility for any loss suffered by any persons resulting from entering into transactions on the Internet irrespective of whether Council facilities are used for the purpose. This includes placement of debit / credit card orders.
- If you purchase personal goods or services via the Council's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.
- You should ensure that personal goods and services purchased are not delivered to Council property. Rather, they should be delivered to your home or other personal address.
- Employees may use the Internet to access social networking sites, such as Facebook. However, as stated above, such activities must only take place outside of working time.
- The use of gambling web sites, or the placing of bets via the Internet or e-mail, is **prohibited** at all times.
- Employees must not subscribe to or enter "money making" sites or enter or use "money making" programs.
- Employees and Councillors must not use Council owned Internet facilities to run a private business.
- Employees and Councillors must not create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive. (See section 6.4)

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Warwick District Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

7.3 Social Media

For the definition of social media, please refer to this policy's definition section.

7.3.1 Personal Use (Blogs, wikis, social networking, etc.)

Social Media provides a number of benefits in which staff and members may wish to participate. For example, social media can be used for rediscovering old school friends on Facebook or keeping up with other people's daily lives on Twitter. However, with the ever-changing realm of social media, it is vital that employees and members understand developments in this arena, as there may be unforeseen consequences when using personal social media accounts; one of the aims of this policy is to give employees and members the information they need to protect both the Council and themselves.

If an employee or member identifies themselves, or can be identified, as working for, or as a representative of, Warwick District Council on any social media or internet presence, that isn't directly controlled and authorised by the Council, then the employee has a responsibility to carry the spirit of this policy into their personal life. A breach of this policy using personal devices away from the work place can amount to gross misconduct.The Council recognises that many employees and members make use of social media in a personal capacity. While they are not acting on behalf of the organisation, employees and members must be aware that they can damage the Council if they are recognised as being one of our employees or a Councillor.

Employees and members are allowed to say that they work for the Council, which recognises that it is natural for its staff sometimes to want to discuss their work on social media. However, the employee's or members'online profile (for example, the name of a blog or a Twitter name) must not contain the Council's name.If employees or membersdo discuss their work on social media (for example, giving opinions on their specialism or role within the Council),they must include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of my employer." However, this only offers very limited protection and it will not be a defence if you have potentially brought WDC, its clients, customers or associated organisations into disrepute.

Remember employees and members are personally responsible for any content they publish, even if it was only intended for a small discreet audience. It is important to check your personal privacy settings to understand who can see the information published, but be aware that privacy settings will not necessarily safeguard you against disciplinary action. Furthermore, even with privacy settings in place what you say can be distributed wider as friends can make comment and then you could be indirectly bringing the Council into disrepute.

The use of social media (blogs, wiki's, twitter, Facebook, etc.) by employees or members whether using Warwick District Council's property and systems or private computer systems, is also subject to the terms and restrictions set forth in this policy.

- Limited and occasional use of the Council's systems to engage in social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate this policy, is not detrimental to the Council's best interests, and does not interfere with an employee's regular work duties.
- Employees/Members must not use social media in a way that may harm or tarnish the image, reputation and/or goodwill of Warwick District Council and/or any of its

employees. Employees/Members are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social media or otherwise engaging in any conduct prohibited by the Council's Dignity at Work Policy irrespective of whether they are at work or at home.

- Employees/Members must not breach confidentiality by revealing information owned by the Council, disclosing personal information about individuals including citizens, or discussing the Council's internal workings.
- Employees/Members must not attribute personal statements, opinions or beliefs to Warwick District Council when using social media. If an employee/member is expressing his or her beliefs and/or opinions, the employee/member may not, expressly or implicitly, represent themselves as an employee or Councillor of Warwick District Council.
- Warwick District Council, logos and any other Council intellectual property must not be used in connection with any social media activity unless officially authorised by an appropriate Head of Service.
- Employees assume any and all risk associated with social media.

A breach of any part of this policy will be regarded as misconduct to which Warwick District Council's Disciplinary Procedure applies and which may lead to dismissal and may also result in legal claims against you and the Council.

During the investigation of any incident, WDC will take into account many factors in assessing whether dismissal is appropriate. Such factors include:

- the nature and severity of the comments made by an employee
- the subject matter of those comments
- the extent of the damage caused to an employer's reputation
- the severity of the damage that could potentially have been caused
- whether there has been a breach of confidentiality
- whether the comments made by an employee were made during working hours and/or using the employer's equipment
- whether there are any other mitigating factors.

Further guidance on this is available through the *Social Media, Discrimination & the Law* training course. Course dates can be found in the Learning & Development guide.

7.3.2 Council related Social Media Usage

For guidelines on the use of social media for official Council business please refer to the Council's Social Media Policy.

7.3.3 Councillor usage of Social Media

Social media is an effective way for elected members to engage with their residents, keep in touch with developing trends across the district and share news from the Council and other organisations that may be relevant to their followers.

It's important to separate your personal life and your role as a Councillor in order to maintain appropriate boundaries. Though your personal life and views may influence your role as a

councillor, it is highly recommended that you maintain this separation so that the lines do not become blurred. Therefore, if you are looking to use social media in your role as a councillor, you must create a *separate* account in order to maintain this separation.

If you are setting up a social media profile for your role as a Councillor, it is standard practice to start your name with the abbreviated 'Cllr' as this will indicate that you are using the account in conjunction with your role.

This doesn't mean that you can't add a personal touch when using your councillor profile. People will want to see your personality, so there's nothing wrong with sharing your views on films, TV programmes, music, sport or any other subject you're passionate about. Just remember: all of your activity must adhere to the Member's Code of Conduct.

As a councillor, you are always perceived to be acting in an official capacity even though you may not be – public office is perceived to be a 24/7 job, so though you may be "off the clock", any comments or posts you share will be perceived to be in your professional capacity.

If you provide delegated access to a party member, assistant or anyone that will be using your account to post on your behalf, you are still responsible and accountable for any content that is posted in your name.

The Member's Code of Conduct extends to your use of social media, therefore your actions on social media must follow the code of conduct, namely:

- Integrity
- Objectivity
- Accountability
- Openness
- Honesty

Further guidance and advice is available in the *Social Media Guide for Elected Members*.

7.4 Downloading

When using the Internet the following must be adhered to:

- Job-related documents, spreadsheets, pdf's, etc. may be downloaded.
- Downloading of programs is prohibited. If required for work purposes, downloading of programs will be carried out by ICT Services because of the high risk of infecting a system with a virus or contravening software licensing.
- Downloading games or other non-work related items to Council equipment is prohibited.

7.5 Offensive, Illegal, Pornographic and Sexually Explicit Material

Offensive material is anything that is pornographic, involves threats or violence, promotes illegal acts, racial or religious hatred or discrimination of any kind.

Anyone using Council equipment to access, send or intentionally receive such material will face serious disciplinary action. If illegal material is accessed, the Council will inform the police and criminal action may follow.

It is possible when accessing a harmless site that links are automatically made to other sites or pages which could be inappropriate. Anyone accessing such sites accidentally should inform their line manager immediately and/or ICT Services. Accidental access will not result in disciplinary action, but failure to report it could do so.

Any user who accidentally encounters offensive material on the Internet, or witnesses the accessing of offensive material must report the incident immediately to their line manager or ICT Services.

Individuals who bring their own laptops, tablets or phones into the workplace containing illegal or offensive material will be treated in the same way as those using Council equipment. Similarly, those who use their own equipment to connect to the Council's network remotely and who use that connection in this manner will be treated in the same way as those using Council equipment.

On occasions staff or Members may need to access inappropriate sites in undertaking their duties, but before doing so they should obtain permission in writing from their Deputy Chief Executive or the Chief Executive. ICT Services Helpdesk must be informed to setup specific access rights. Each site visited should be recorded in a log which identifies the site and the date and time of the visit. The log will be reviewed regularly by the Information Security Officer.

Except in these circumstances there can be no possible legitimate Council use for accessing or transmitting sexually explicit materials at work. The accessing, viewing, downloading, storing or printing of any content of an illegal, pornographic or sexually offensive nature is expressly forbidden and will be treated as gross misconduct leading to summary dismissal for staff or, for Members, to a report to the Standards Committee.

7.6 Blocked Web Sites / Content

For legitimate business reasons, staff or members may require access to web sites which are blocked as a result of the Council's corporate proxy configuration settings. To unblock a web site for business reasons, either temporarily or permanently, a request should be made to the ICT Services' Helpdesk.

If a web site is blocked and is only required for personal use, the site will remain blocked. This will limit ICT resources being unnecessarily diverted to deal with non-work related matters and will also reduce the complexity of the Proxy server rule set.

7.7 Connecting to the Internet

Access to the Internet for web browsing is enabled through the Council's central gateway and its associated Firewalls and virus detection facilities. Access to the Internet for web browsing, other than through the gateway, can only be authorised by the ICT Services Manager. Any member of staff or Member found connecting Council equipment directly to the Internet for web browsing will be subject to disciplinary action.

7.8 Copyright Compliance

Information in electronic form may be subject to the Copyright, Designs and Patent Act 1988. This requires that you get permission from the owner of such before making use of it in any way. The council has a CLA copyright license which permits employees (which includes temporary staff and contractors) to download, copy and reuse copyrighted material subject to license conditions.

The CLA license only covers council employees and therefore **does not** cover Members.

Users should not copy information originated by others and re-post it without permission from, or at least acknowledgement of, the original source, even if the content is modified to some extent. Users should not assume that information posted on the internet actually originates from the person or organisation that appears to have produced it without some form of authentication.

Copyright and other rights in all messages posted on the internet from a council account, such as material produced at work, belongs to the council, and not to users personally.

8 Policy Compliance

Any breach of this policy by staff may lead to disciplinary action being taken and, in cases of gross misconduct, termination of employment without notice. Some cases may result in the Council informing the police and criminal action may follow. For Members, references in this policy to disciplinary action will mean referral to the Standards Committee and this document will be treated as a local protocol for this purpose. Any breach of this policy by suppliers will be subject to appropriate action by the relevant Deputy Chief Executive.

Should the Council be sued due to misuse of Council ICT equipment or the actions of a user which contravene this policy, the Council reserves the right to claim damages from the authorised user concerned.

9 Policy Governance

The following table identifies who within Warwick District Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Accountable	Deputy Chief Executive
Responsible	ICT Services Manager
Consulted	ICT Steering Group, Human Resources, CMT, Trade Unions & Employment Committee
Informed	All Council personnel, temporary / agency staff, contractors, consultants, suppliers and Members.

10 Review & Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Council's Information Security Officer.

11 References

The following Warwick District Council policy documents are relevant to this policy:

- Warwick DC – Monitoring Policy
- WDC Online Social Networks Policy (Web Site Manager)

12 Key Messages

The Council monitors the use of all of its ICT Equipment, including the use of the Internet. You should be aware that this monitoring may reveal personal information about you, for instance which websites you visit etc.

- Provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for example during your lunch-break).
- Users are responsible for ensuring that no other user connects to the Internet using their logon details.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Individuals who bring their own laptops, tablets or phones into the workplace containing illegal or offensive material will be treated in the same way as those using Council equipment.
- The use of gambling web sites, or the placing of bets via the Internet or e-mail, is prohibited at all times.
- Users must not download games or other non-work related items to Council equipment.

- Users must not use blogs, wikis or social networking sites etc to make discriminatory, disparaging, defamatory or harassing comments about employees of the council, or use the Internet in any other way which may contravene the Council's Dignity at Work Policy.
- Employees and members are personally responsible for any content they publish, even when using personal devices. Therefore the employee has a responsibility to carry the spirit of this policy into their personal life. A breach of this policy using personal devices away from the work place can amount to gross misconduct.
- You must respect the legal protections to data and software provided by copyright and licences.