



Policy on the use of Internet, social media and email systems by Officers, Employees and Councillors Prohibited Activities

The following activities are expressly prohibited and this list is not exhaustive.

Councillors, Officers and employees using the Internet, social media and email must not:

Communication

- Communicate or distribute libellous or defamatory material about any individual, firm, body or organisation, including the Council by email or Social Media;
- Claim to represent the views of the Council unless authorised to do so.
- Transmit confidential or sensitive information relating to individuals or any aspect of the Council's business over the internet, social media sites or via e-mail
- Publish material or a comment that could undermine public confidence in the Council or misrepresent the Council and its services
- Manipulate dialogue or attempt to control people's points of view
- Publish untrue statements about another person which could damage their reputation or working relationships
- Post comments to newsgroups or chat rooms on Social Media on behalf of the Council unless authorised to do so

Inappropriate Behaviour

- Knowingly accessing or attempting to access inappropriate Internet sites, download, store or circulate material which is illegal or inappropriate to the role of a Councillor. Inappropriate in this context includes sites or material which are for example, pornographic, racist, or sectarian, involve illegal activity, or other actions that contravene the Council's disciplinary code or breaches the Councillor Code of Conduct
- Send inappropriate messages/create posts which breach the standards and values set out within the Council's Equal Opportunities Policy or which are otherwise abusive, threatening or provocative.



Legislation

- Download, possess, distribute or copy works (e.g. document, photograph, piece of music or video) without the consent of the copyright owner;
- Disclose personal data or information about any individual/colleague/service user which could be in breach of the Data Protection Act 1998
- Give out personal details of employee's telephone number, home address, personal email address, without checking whether the person requesting the information is entitled to receive it and the employee gives consent to the disclosure

General

- Purchase goods or services, or conduct other transactions over the Internet in the Council's name without proper authorisation in accordance with relevant Council procedures in force at the time e.g. rules governing e-procurement;
- Use the Council's systems for political party activity;
- Use the Council's systems for conducting a private or commercial business undertaking;
- Use the Council's Internet system for the purpose of online gambling or e-auctions (e.g. Online Bingo, E-Bay);
- Subscribe or register to personal newsgroups, shopping or social media sites using the Council's Tablets
- Download software or accept cookies associated with personal online transactions e.g. iTunes, Napster, Amazon wish list etc. on the Council's Tablets
- Participate in any activity that could cause congestion and disruption of network systems. This includes sending and forwarding unsolicited or inappropriate e-mail (known as 'spam') to groups or mailing lists, participating in chain or pyramid letters or similar schemes or making other excessive use of unsolicited e-mail;
- Use the Council's Tablets for on-line game playing or chat lines.



- Post videos or pictures of others Officers, employees and Councillors without their permission
- Use the Council's logo on personal web pages or social media sites.